Table of Contents

General **2**
G Data PremiumHotline 2
PremiumSupport extensions 2
Licence agreement 2

Prior to installation **6**
System requirements 6
Boot scan 6

Installation **11**

G Data AntiVirus ManagementServer **13**
Installation of the ManagementServer 13

G Data AntiVirus Administrator **18**
Installation of the Administrator 18
Logon 18
Initial program launch (Setup wizard) 18
Other program starts (access password) 18
Administrator program setup 18

G Data AntiVirus Client **70**
Installation of the clients 70
Security icon 70

G Data AntiVirus WebAdministrator **75**
Installation of the WebAdministrator 75
Program setup of the WebAdministrator 75

Attachment **77**
Troubleshooting (FAQ) 77

General

In these days of global networking and the massive security risks this incurs, the subject of *virus protection* is no longer one just for IT specialists. Rather it has to be considered within the context of comprehensive, company-wide risk management at the highest level of management. Computer network downtime caused by a virus strikes a company where it is most vulnerable. The result: Cessation of business-critical systems, loss of success-related data, loss of important communication channels. Computer viruses can cause damage to a company that it can never recover from!

G Data AntiVirus provides you with high-end virus protection for your entire network. For years its leading security capabilities have been awarded terrific scores in numerous tests. *G Data AntiVirus* is based on central configuration and administration plus as much automation as is possible. All clients, whether they are workstations, notebooks or file servers, are controlled centrally. All client processes run invisibly in the background. Automatic Internet updates enable extremely fast reaction times in the event of virus attack emergency. Central control with the *G Data AntiVirus ManagementServer* makes installation, settings, updates, remote control and automatic systems possible for the entire network. This reduces the workload on the system administrator and saves time and money.

Your *G Data Security Team*

G Data PremiumHotline

The ***PremiumHotline*** for your *G Data AntiVirus multi-user and network licences* is available at any time for all registered business customers.

www.gdata-software.com

Your ***registration number*** is located on the back of the user manual. If you bought the software online, you will receive your registration number in a separate email. You can enter it via the ***online registration form***. You will then immediately be given a password online with which you can download your personal Internet updates. The ***Online database for frequently asked questions (FAQ)*** already contains answers to many questions concerning *G Data AntiVirus.* Before contacting the ***hotline***, please check your computer/network configuration. The following information is particularly important:

- the ***version numbers*** for the Administrator and the ManagementServer (you will find these in the ***Help*** menu of the Administrator software)
- the ***registration number*** or the ***user name*** for the ***Internet update***. The registration number is located on the back of the user manual. The user name is sent to you during ***online registration*** .
- exact Windows version (Client/Server)
- other installed hardware and software components (Client/Server)

These details will make the call to the hotline representative faster, more effective and more successful. If at all possible, please ensure that the telephone is in the vicinity of a computer on which the Administrator software for the ManagementServer has been installed.

PremiumSupport extensions

With ***PremiumSupport*** once you have carried out your Online registration you will receive hourly updated virus data by Internet update for a year so that your virus countermeasures are always optimised. In addition you will receive detailed information (e.g. about upgrades to the ManagementServer software and current virus warnings) by email. PremiumSupport can be terminated or extended with a time limit or indefinitely. Please contact us at

www.gdata-software.com

? Of course our ***Business Sales*** department is here to help and will be happy to provide you with individual advice. Please understand that technical questions about existing software can only be handled by our ***ServiceCenter*** .

Licence agreement

The following are the contractual terms and conditions for the use of the *software* ***G Data AntiVirus*** by the end user (hereafter also called: Licencee).

1. Object of the contract: The object of the contract is the *G Data software* recorded on a data medium or downloaded from the Internet and the program description. This is hereafter referred to as Software. *G Data* calls attention to the fact that, due to the status of technology, it is not possible to manufacture Software in such a way that it operates without error in all applications and combinations.

2. Scope of use: *G Data* grants you, for the duration of this contract, the simple, non-exclusive and personal right (hereafter referred to as Licence) to use the Software on a contractually agreed number of computers. The Software can be used in the form of an

installation on a physical unit (CPU), a virtual/emulated machine (such as VMWare) or an instance of a terminal session. If this computer is a multiple user system, this usage right applies to all users of this one system. As the Licencee you are permitted to transfer the Software from one computer to another in physical form (i.e. stored on a data medium), provided that it is not used on more than the contractually agreed number of computers at any time. Use that exceeds this is not permitted.

3. Specific limitations: The Licencee is prohibited from changing the Software without the prior written consent of *G Data*.

4. Ownership of rights: When purchasing the product you only receive ownership of the physical data medium onto which the Software has been recorded and to updates agreed in the context of support. Purchase of rights to the Software itself is not included with this. *G Data* especially reserves all publication, reproduction, processing and usage rights to the Software.

5. Reproduction: The Software and associated written materials are protected by copyright. Creation of a backup copy is permitted, as long as this is not passed on to a third party.

6. Duration of the contract: The contract is granted for an unspecified period. This duration does not cover the procurement of updates. The Licencee's right to use the Software expires automatically and irrevocably if he breaches any of the terms of this contract. On termination of the usage right it is obligatory that the original CD-ROM including any UPDATES/UPGRADES and any written materials is destroyed.

7. Compensation for breach of contract: *G Data* calls attention to the fact that you are responsible for all damages through breach of copyright that *G Data* incurs from breach of the terms of this contract by you.

8. Changes and updates: Our most recent service terms and conditions shall always apply. The service terms and conditions may be changed at any time, without notice and without giving reasons.

9. *G Data* warranty and liability:

a) *G Data* guarantees with respect to the original Licencee that, at the time of delivery, the data carrier (CD-ROM) onto which the Software has been recorded is error-free under normal conditions of use and within normal maintenance conditions for material performance.

b) If the data medium or download from the Internet is faulty, the purchaser is entitled to demand delivery of a replacement during the warranty period of 6 months from delivery. To do so, he must provide proof of purchase of the Software.

c) As per the reason previously stated in para. 1, *G Data* accepts no responsibility for the Software not being error-free. In particular, *G Data* accepts no warranty for the Software meeting the purchaser's requirements and purposes or working in conjunction with programs selected by him. The purchaser is responsible for proper selection and consequences of use of the Software, together with its intended or achieved results. The same is true of written materials related to the Software. If the Software is essentially unusable in the sense of para. 1, the purchaser has the right to revoke the contract. *G Data* has the same right if manufacture of Software that may be required in the sense of para. 1 is not possible within reasonable cost limits.

d) *G Data* is not liable for damages unless damage is caused intentionally or by gross negligence on the part of *G Data*. Liability for gross negligence does not extend to sales persons. The maximum award for damages shall be the purchase price of the Software.

10. Legal domicile: The exclusive legal domicile for all disputes directly or indirectly arising from this contract is the registered head office of *G Data*.

11. Final provisions: If individual provisions of this Licence Agreement become invalid, the remaining provisions stay in force. In place of the invalid provision, an effective provision that approximates its commercial intention as closely a possible shall be considered as agreed upon.

? *Copyright © 2009 G Data Software AG*

Engine A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2009 BitDefender SRL.

Engine B: © 2009 Alwil Software

OutbreakShield: © 2009 Commtouch Software Ltd.

[G Data AntiVirus - 06.05.2009, 14:46]

Prior to installation

In the event of an acute virus threat please first run a ***Boot scan*** on the affected computers.

- Then install the ***ManagementServer*** on your server. Please note that the ManagementServer can only be installed and run on a Windows Vista, Windows XP Professional or Windows 2003 server system. When installing the ManagementServer the ***Administrator*** is automatically installed on the server. You can use this program to manage the ManagementServer from the server computer. To guarantee optimal protection, the computer should always be accessible (switched on) and available for automatically loading virus signatures via an Internet connection. Therefore, it is not absolutely necessary to install the ManagementServer on your central file server.
- Now carry out the ***online registration***. You cannot update the virus databases via the Internet without registering online.
- When the Administrator is first started on the server, the ***Setup wizard***. also starts. You can use this to install the ***client software*** directly onto the clients you want in your network without having to carry out the installation on each computer individually.
- If problems should occur during ***remote installation*** on the clients, you can of course also install the client software on the clients manually or semi-automatically. To ensure that your server is also protected against virus threats, you should of course also install the client software on your server.
- Now you can run virus prevention and countermeasures as well as Internet updates for *G Data AntiVirus client and server software* easily and centrally via the Administrator, by, for example, using the ***G Data AntiVirus monitor*** for continuous checking or for defining scan jobs that your network regularly runs to detect any possible viruses.
- If you should need to solve a problem *on site*, you can install the Administrator software quickly and easily on any client and also have complete access to the ManagementServer from there.

System requirements

The *G Data AntiVirus system* builds upon the ***TCP/IP protocol*** and uses this both for communication between client and server computers among each other as well as for the online connection to the *G Data UpdateServer*. The following minimum requirements apply both to clients and or server:

- ***G Data AntiVirus ManagementServer***: PC with Windows Vista, XP, or Server 2003 (preferably the server versions, also x64 Edition), at least 128 MB RAM, Internet access
- ***G Data AntiVirus*** Clients: PC with Windows Vista, XP, 2000 or Server 2003 (also x64 edition), at least 256 MB RAM

? For ***Linux computers*** that operate as file servers and provide Windows authorisations to different clients (via the ***SMB protocol***), a module can be manually installed that controls access to the cleared areas and carries out a file scan with every access event, so no malware can migrate from the ***Samba server*** to the Windows clients (or vice versa).

Boot scan

The ***boot scan*** will help you fight viruses that have embedded themselves prior to installation of the antivirus software on your computer and that may prevent the ***G Data software*** from being installed. That is why there is a special version of the ***G Data software*** that can be run before the start of Windows.

? ***What do I do if my computer will not boot from the CD-ROM?***

If your computer will not boot from the CD/DVD-ROM, you may need to set this option up first. This is done in the so-called ***BIOS***, a system that is automatically started before your Windows operating system. To make changes in BIOS, proceed as follows:

1. Switch your computer off.
2. Restart your computer. Usually you reach the BIOS setup by pressing the ***DEL*** button as the computer is booting up (and sometimes the ***F2*** or ***F10*** button as well).
3. How to change individual settings in your BIOS setup varies from computer to computer. Please consult your computer's documentation. The result should be the boot sequence ***CD/DVD-***

ROM:, C: , meaning that the CD/DVD-ROM drive becomes the ***1st boot device*** and the hard disk partition with your Windows operating system on it becomes the ***2nd boot device***.

4. Save the changes and restart your computer. Your computer is now ready for a boot scan.

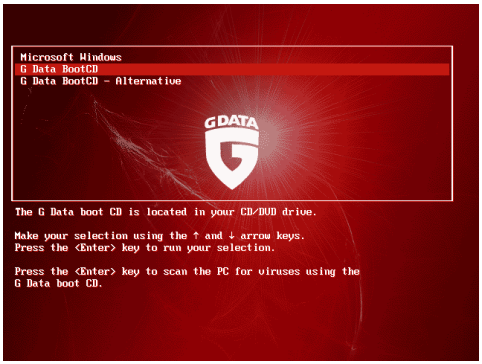
For the ***boot scan*** itself, proceed as follows:

1a ***Boot scan using the program CD***: Use the ***G Data program CD*** to boot up your computer. - Insert the ***G Data software CD*** into the drive. In the start window that appears, click on Cancel and switch the computer off.

1b ***Boot scan with G Data software that you have downloaded from the Internet***: Use the Create BootCD option in the ***G Data software program group*** to burn yourself a new boot CD. - Insert the boot CD you have burnt into the drive. In the start window that appears, click on Cancel and switch the computer off.

After this first step the boot scan in all three scenarios will proceed identically:

2 Restart the computer. The ***G Data boot scan*** start menu will appear.


Microsoft Windows
G Data BootCD
G Data BootCD - Alternative
GDATA
The G Data boot CD is located in your CD/DVD drive.
Make your selection using the ↑ and ↓ arrow keys.
Press the <Enter> key to run your selection.
Press the <Enter> key to scan the PC for viruses using the
G Data boot CD.

3 Use the arrow keys to select the G Data BootCD option and confirm your choice by pressing **Enter**. A Linux operating system is now started from the CD and a ***G Data special version*** for boot scans appears.

? If you have problems displaying the program interface, restart the computer and select the G Data BootCD - Alternative option.

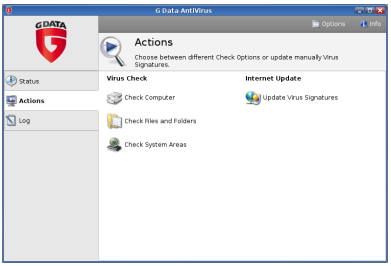
4 The program will now suggest updating the virus definitions (or ***virus signatures***).

G Data AntiVirus
Warning
G Data AntiVirus detected that virus signatures files are outdated and recommends an update.
Whould you like to perform an update now?
No
Yes

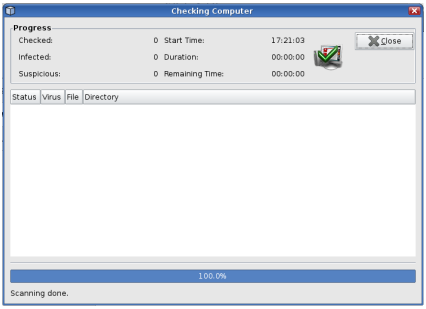
5 Click on Yes and run the update. As soon as the data has been updated via the Internet, you see the message ***Update complete***. Now exit the update screen by clicking the **Close** button.

? The automatic ***Internet update*** is available if you are using a ***router*** that assigns IP addresses automatically (***DHCP***). If the Internet update is not available, you can still perform the ***boot scan*** using old virus signatures. However, in that case, you should perform a new boot scan with updated data as soon after installing the ***G Data software*** as possible.

6 You will now see the program interface. Click on the Check Computer entry; your computer will now be scanned from viruses and malware. Depending on the type of computer and size of the hard drive, the boot scan can take an hour or more.



7 If the ***G Data software*** finds any viruses, please use the options provided in the program to remove them. Once the virus has been removed successfully, the original file is available again.



8 Once the virus check is complete, exit the system by clicking the ***Exit*** button and then selecting `Restart` .

The ***Exit*** button is located on the bottom right of the Linux program interface.

9 Remove the ***G Data Software CD*** from the drive as soon as your drive tray opens.

10 Switch off your computer again and restart it. Your computer will now start with your usual Windows operating system again (that is, Windows XP or Windows Vista), and you can be certain of being able to install the standard ***G Data software*** on a virus-free system.

Installation

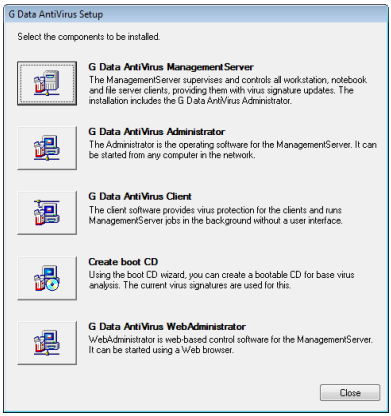
Installation of the *G Data AntiVirus Windows version* is particularly easy. Simply start Windows and place the *G Data AntiVirus CD-ROM* in the CD-ROM drive. An installation window will open automatically.

? If you have not activated the ***Autostart function on your CD-ROM drive***, *G Data AntiVirus* will not be able to start the installation process automatically. In the Windows ***Start menu***, click ***Run***, enter ***e:\setup.exe*** in the window displayed and click ***OK***. This will then open the welcome screen for *G Data AntiVirus installation*. The ***e:*** signifies the drive letter designation for your CD-ROM drive. If your CD-ROM drive is set up under a different drive character designation, please enter the relevant letter instead of ***e:***. .

Please close all other programs before beginning to install *G Data AntiVirus*. Errors or cancellation could occur if, for example, programs are left open that access data *G Data AntiVirus* requires for the installation.

- **Install**: Click on this button to start installing *G Data AntiVirus* on your computer
- **Browse**: Here you can view the CD-ROM directories via Windows Explorer.
- **Cancel**: Clicking on this will let you close the Autostart window without having to perform any actions.

After you have clicked on the button **Install**, a screen appears in which you select which of the *G Data AntiVirus components* you want to install.


G Data AntiVirus Setup
Select the components to be installed.
G Data AntiVirus ManagementServer
The ManagementServer supervises and controls all workstation, notebook and file server clients, providing them with virus signature updates. The installation includes the G Data AntiVirus Administrator.
G Data AntiVirus Administrator
The Administrator is the operating software for the ManagementServer. It can be started from any computer in the network.
G Data AntiVirus Client
The client software provides virus protection for the clients and runs ManagementServer jobs in the background without a user interface.
Create boot CD
Using the boot CD wizard, you can create a bootable CD for base virus analysis. The current virus signatures are used for this.
G Data AntiVirus WebAdministrator
WebAdministrator is web-based control software for the ManagementServer. It can be started using a Web browser.
Close

The following installation options are available:

- **G Data AntiVirus ManagementServer**: First of all the ***ManagementServer*** should be installed on the computer you want to use as the antivirus server. The ManagementServer lies at the heart of the *G Data AntiVirus architecture*: It administers the clients, automatically requests the latest software and virus signature updates from the *G Data UpdateServer* and controls the AntiVirus technology in the network. When the ManagementServer is installed, the ***administrator software*** on the server that you can use to administer the ManagementServer is automatically called.
- **G Data AntiVirus Administrator**The ***Administrator*** is the control software for the ManagementServer which - centrally controlled by the system administrator - secures the entire network. The Administrator can be started using password protection from any computer running Windows.
- **G Data AntiVirus Client**: The ***client software*** provides the virus protection for the clients and runs ManagementServer jobs in the background without a user interface. Installing the client software is generally done centrally by the Administrator for all clients.
- **Create boot CD**: The Boot-CD wizard can be used to create a bootable CD for basic scanning of your computer prior to starting the Windows operating system. Current virus signatures are used for this. You can use the Boot CD to run a ***Boot scan***, even without the original *G Data AntiVirus software CD*. Please also refer to the section ***Boot scan***.
- **G Data AntiVirus WebAdministrator**: The ***WebAdministrator*** is web-based administration software for the ManagementServer. It can be launched via a web browser.

? Directions and information that you should observe during the installation can be found in the sections for the respective software components.

G Data AntiVirus ManagementServer

The ***ManagementServer*** lies at the heart of the *G Data AntiVirus architecture*: It administers the clients, automatically requests the latest software and virus signature updates from the *G Data UpdateServer* and controls the virus technology within the network. For communication with the clients, the ManagementServer runs over ***TCP/IP***. For ***Clients*** that are offline, the jobs are automatically collected and synchronised with the next online session. The ManagementServer possesses a central ***Quarantine*** folder to which you can optionally allow suspicious files to be encrypted and saved, then subsequently deleted, disinfected or, where applicable, routed to the ***Emergency AntiVirus service***. The ManagementServer is controlled via the ***administrator software***.

? If you close the administrator software, the ManagementServer does not close. This continues to remain active in the background and controls the processes that were set by you for the clients.

Installation of the ManagementServer

To install the ***ManagementServer*** you require at least Windows Vista, a Windows XP or Windows 2003 server. Insert the *G Data AntiVirus CD-ROM* and press the **Install** button. Then select the **G Data AntiVirus ManagementServer** components by clicking on the adjoining button.

Start screen

In the following start screen, you are informed that you are about to install the ManagementServer on your system. Please ensure that you have now closed all open applications in your Windows system, as otherwise they may cause problems during the installation. Click on **Next** to continue with the installation.

Licence agreement

Please read the Licence Agreement regarding use of the software, then select **I accept the terms of the licence agreement** and click on **Next** if you agree with the terms in this document.

Target folder

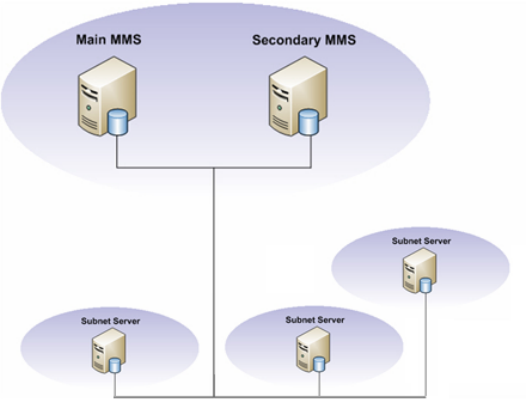
The next screen allows you to select the location in which the data of the ManagementServer should be saved. If you wish to select a separate target folder, then by clicking the button **Change** you can open a directory tree view in which you can select another directory or create a new one.

Select server type

When selecting a server type you have the following options:

- **Install a main server**: It is essential that the *G Data AntiVirus ManagementServer* is created as the ***main server*** (***main MMS***). The main server represents the central configuration and administration entity of the network-based virus protection architecture. The ManagementServer provides the computers to be protected with the latest virus signatures and program updates. In addition, all specific client settings are carried out centrally on the ManagementServer.
- **Install a secondary server**: When using an ***SQL database*** it is possible to run a ***second server*** (***secondary MMS***), which uses the same database as the main server. If the ***main server*** is unavailable for an hour or more, the clients connect automatically to the secondary MMS and load signature updates from it. They switch back to the main server as soon as it is available again. Both servers load the signature updates independently of each other.
- **Install a subnet server**: With large networks, it is also useful to operate the *G Data AntiVirus ManagementServer* as a ***subnet server***. Subnet servers serve to reduce the network traffic loading between clients and the main MMS. They can be used in subnetworks where their task is to manage the clients allocated to them. The subnet servers remain fully functional, even if the main or secondary ManagementServer is inaccessible.

Schematically therefore, the ***structure of the server types*** in large networks appears as follows: Subnet servers bundle together individual clients or client groups and pass these on to the main server. The latter is supported by a secondary server, which should the main server fail, functions as a backup.



Database server

Please select a database server that you will install now. You have the option of using existing ***SQL servers***, ***Microsoft SQL Express*** or an ***integrated database*** (e.g. for smaller networks).

? A server operating system is not absolutely necessary. The SQL variant is provided primarily in larger networks with a client number of > 50.

? With the installation of Microsoft SQL Express, a possibly still existent *conventional* database is automatically converted.

Computer name

Now check the ***name of your computer*** on which you are installing the ManagementServer. This computer must be addressable by the clients in the network via the name given here. If the correct name is not given here, please change the specification under **Name** accordingly.

Starting the installation

The ManagementServer will now be installed. The installation starts with a completion screen. Click on **Install**.

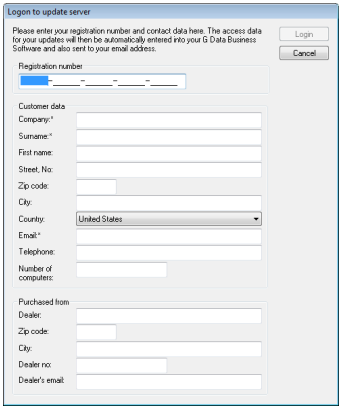
Online registration

No later than prior to carrying out ***Internet updates*** you must have registered with the *G Data UpdateServer* to receive your access data. For this, you can register directly during the installation or later by executing the function **Internet update** under ***Start > Programs > G Data AntiVirus ManagementServer***. Use the **Online registration** button here. You will then be asked for your customer data and registration number.

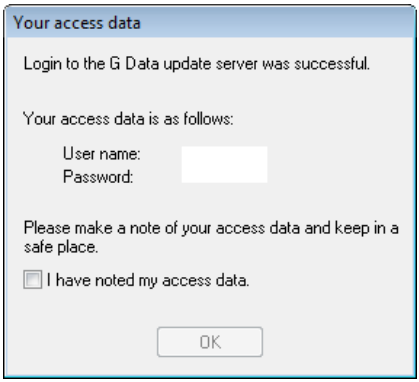
? You will find your ***registration number*** on the back of the user manual. If you bought the software online, you will receive your registration number after the order in a separate email.

? Please note of course that a permanent or automatic-dial ***Internet connection*** must be available or able to be set up.

Enter the registration number as it is, without spaces or hyphens, in the relevant 5-character entry fields. Please also ensure that all other entry fields are correctly completed, as online registration can only be completed using all the data requested here.



Immediately after online registration, you will receive your user name and your password in an information box.


Your access data
Login to the G Data update server was successful.
Your access data is as follows:
User name:
Password:
Please make a note of your access data and keep in a safe place.
I have noted my access data.
OK

? ***Warning***: Always keep your ***user name*** and ***password*** in a safe place, so you still have it in the event of a possible reconfiguration of your computer. You can proceed with the program after checking off the checkbox with the corresponding prompt.

? *G Data AntiVirus* carries out these tasks automatically in the Internet update form. You can now run Internet updates.

? The ***Internet updates*** can be run directly from the Administrator interface and even automated to run at freely configurable frequencies.

Database type configuration

This installation step only occurs if you reinstall the ManagementServer or if an ***SQL database*** is already installed on the computer. Usually it is sufficient to close this info box by clicking on the **Close** button.

Installation completion

After installation and after each computer restart the ManagementServer will now start automatically. To carry out changes to the ManagementServer, go to ***Start > (All) Programs > G Data AntiVirus ManagementServer*** and select the ***G Data AntiVirus Administrator*** option. This will start the administration tool for the ManagementServer.

G Data AntiVirus Administrator

The ***administrator*** is the control software for the ManagementServer which - centrally controlled by the system administrator - secures the entire network. The Administrator can be started from any computer running Windows using password protection. All conceivable virus scanner services such as automatic installations, software and virus signature updates, virus analyses (immediate or periodic), monitor functions and changes to settings are possible company-wide as remotely controlled jobs. You can invoke the administrator tool for the control of the ManagementServer by clicking the entry ***G Data AntiVirus Administrator*** in the program group ***Start > (All) programs > G Data AntiVirus ManagementServer*** from the start menu.

Installation of the Administrator

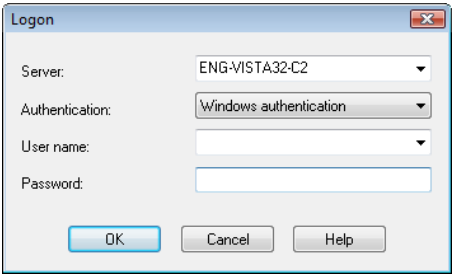
When installing the ***ManagementServer*** the ***Administrator*** is also installed automatically on the same computer (i.e. the computer you want to use as the ***server***). Therefore you do not need to install the Administrator separately. However the Administrator can also be installed on every client computer (independent of its installation on the server). Thus you can also manage the ManagementServer remotely. To install the Administrator on a client computer, please place the *G Data AntiVirus CD-ROM* in the client computer's CD-ROM drive and press the **Install** button. Then select the component **G Data AntiVirus Administrator** by clicking on the adjoining button.

In the following start screen, you are informed that you are about to install the Administrator on your system. Please ensure that you have now closed all open applications in your Windows system, as otherwise they may cause problems during the installation. Click on **Next** to continue with the installation and follow the installation steps with the help of the installation wizard.

After the installation, you can use ***Start > (All) Programs > G Data AntiVirus ManagementServer*** to select the ***G Data AntiVirus Administrator*** entry and so start the administration tool for the ManagementServer.

Logon

When starting the Administrator, you will be prompted for the **server**, **authentication**, **user name** and **password**.



In the **Server** field, enter the name of the computer on which the ManagementServer was installed.

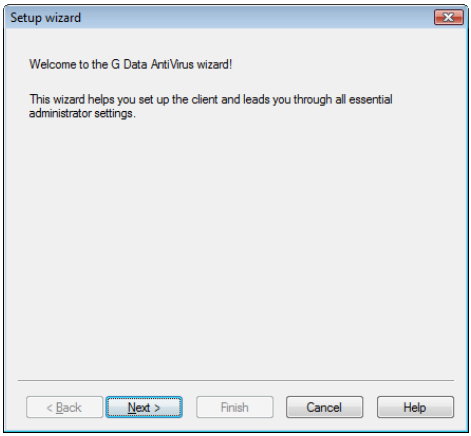
Now select your **authentication**.

- **Windows authentication**: If you select this Authentication variant, you can logon to this computer with the user name and password of your administrator access, i.e. using the ***Windows user account***.

- **Integrated authentication**: Using integrated authentication, you can, as system administrator, also give other people access to the *G Data AntiVirus Administrator*. For example, you can create a special account that only contains read rights. You can create and administer these additional accounts via the function ***User management*** .

Initial program launch (Setup wizard)

When the administrator is first started the ***Setup wizard*** is automatically opened. This helps to set up the clients and takes you through all the necessary settings. After the initial launch, the wizard can still be started at any time via the **Setup wizard** command in the **file** menu.


Setup wizard
Welcome to the G Data AntiVirus wizard!
This wizard helps you set up the client and leads you through all essential administrator settings.
< Back
Next >
Finish
Cancel
Help

Activate

All clients that are to be monitored by *G Data AntiVirus* must first be activated. Select the computers in the list and then click the button **Activate** . Some computers may not be included in the list (e.g. because they have not been switched on for a long time or have not set up file or printer sharing). To activate these clients, you can enter the name in the **Computer** entry field and click the button **Activate** next to the entry field. The computer will then be included in the list. Click on **Next** when you have activated all clients.

Install

In the following dialogue box the checkbox for **Automatically install client software on the enabled computers** is checked. If you prefer to install the software on the client computers manually, please uncheck this box.

Default settings

In the following dialogue you can change the default settings for monitor, virus protection and client settings. The default settings are selected so that they can also be used directly for most networks without change. If these settings are ultimately not optimal for your network, you can naturally change these at any time via the respective administrator work area. Detailed explanations about the adjustable options can be found in the comments for the task area **Settings**.

Internet update

The ManagementServer can load new virus signatures and program files over the Internet. So that this process occurs automatically, login and dial-up (where necessary) must be automated. First enter the ***access data*** here that you received during online registration. A detailed description of scheduling update intervals and the execution of basic settings is contained in the ***Internet update*** section. Of course, you can also automate Internet updates at a later date via the Administrator program interface.

Email settings

The ManagementServer can send potentially infected files to the ***Emergency AntiVirus service*** for investigation. So that this can be done at the push of a button, you need to enter the name of the ***mail server***, the ***port number*** (***SMTP***) and the ***sender address***. Responses from the ***Emergency AntiVirus Service*** will be sent back to this email address.

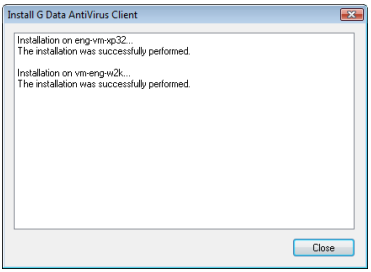
Email notification

The ManagementServer can inform the network administrator via email if a virus is found on one of the clients. Enter the email address for the warning recipient. Use the **quantity limit** to stop your mailbox from being *overloaded* with notifications in the event of a massive virus attack. Click on **Finish** to exit the wizard.

Automatic installation of the client software

If you have selected Client software automatically installed you will be asked to enter a user account on the server that has access rights for the clients.

After confirming the dialogue entries the ManagementServer tries to install the client software on all activated computers. An information screen informs you about the installation progress and any problems.

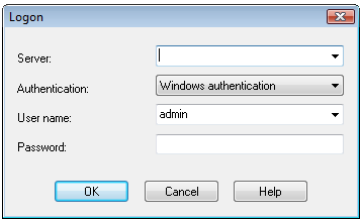


? If problems should occur during ***remote installation*** of *G Data AntiVirus Clients* via the Administrator, you also have the option of installing the client software manually or semi-automatically on the client computers. Please refer to the sections ***Install G Data AntiVirus Client***.

? You can also install special client software on ***Linux clients*** in the network. For more information please read the section ***Installation of the client software on Linux computers*** in the annex of this documentation.

Other program starts (access password)

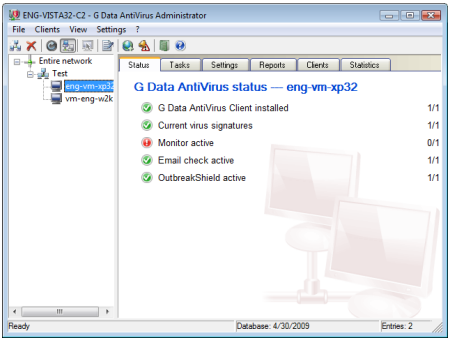
You can invoke the administrator tool for control of the ManagementServer by clicking the entry ***G Data AntiVirus Administrator*** in the program group ***Start > Programs > G Data AntiVirus ManagementServer*** from the start menu. When you start the administrator, you will be asked for the server and password. Enter the name of the computer on which the ManagementServer was installed in the field **Server**.



Now the administrator program interface opens. Its functions are explained in the following sections .

Administrator program setup

The administrator interface is subdivided as follows:



The left ***Client selection area*** shows the hierarchical structure of the monitored computer. To the right of this, one can switch over to the respective ***Task areas*** via tabs. The content of the task area normally relates to the computer highlighted in the client selection area or to the selected group of clients. Above these columns a ***Menu bar*** and ***Toolbar*** for global functions can be seen, which can be used in all fields of activity.

? When administrating ***Linux clients***, which serve as ***Samba servers***, functions, which, for example are involved in handling emails are blocked because these are not required in the context of a file server. Functions which cannot be adjusted for Linux clients are highlighted using a red dot in front of the corresponding function.

Menu bar

The menu bar contains global functions that can be used in all task areas. Tasks are divided into the following areas:

- **File**
- **Clients**
- **View**
- **Jobs** (only in the **Jobs** task area)
- **Reports** (only in the **Reports** task area)
- **Client settings** (only in the **Clients**task area)
- **Settings**
- ***? (Help)***

File

Basic user management and printer functions as well as the ***Setup wizard*** are available to you in the file menu.

Setup wizard

With the Setup wizard, you can select and activate the clients from your network in a user-supported process for which you desire a check to be run by *G Data AntiVirus*. The Setup wizard is explained in detail in the section ***Initial program launch (Setup wizard)*** .

Display log

The ***log file*** provides a quick global overview of the last actions carried out by your *G Data AntiVirus*. All relevant information is displayed here. You can filter the log display using the following setting fields:

- **Log view**: specify here whether you would like to see a log of client or server procedures.
- **Computer/group**: specify here whether you would like to view a log for all clients or groups or only individual areas.
- **Procedure**: Here you can define whether you would like to view all information relevant to the log or only notifications on specific topics.
- **Time**: Specify the from/to time here, for which log information should be available.

The field **Update** is to specify that procedures which occur while the log file view is open are also listed. By clicking **Close** the log file window is closed; moreover you can ***print*** and ***export*** the log or a highlighted area of the log (in XML format). All procedures first appear in a chronological sequence and can be easily sorted according to specific criteria by simply clicking on the respective column title. The column according to which current sorting is carried out, is indicated by a small arrow symbol.

User management

As system administrator you can allocate additional user accesses for the Administrator interface. Click on the **New** button, then enter the user name, the **authorisations** for this user (**Read / write** or **Read only**), define the **account type** (**integrated login**, **Windows user**, **Windows user group**) and enter a **password** for this user.

Manage server

Via Manage server you can assign ***clients*** to individual ***subnet servers***, which then bundle the communication of these clients with the ***main server*** and in this way optimise network use. You can install subnet servers using this menu. By clicking the button **Assign clients**, you can assign the existing clients to the defined subnet servers.

? The allocation of clients to subnet servers is independent from the grouping of clients in respect of virus checking. Clients of different subnet servers can of course be joined together in a group for ***virus checks*** and scan jobs.

Subnet server synchronisation

To enable possible changes even outside the regular communication intervals of server and subnet server, you can also carry out the subnet server synchronisation manually.

Print templates

Here you can undertake comprehensive settings for the printout of log and statistical functions and save them in templates that can be used independently of each other.

> ? Depending on the selected ***field of activity***, you have various selection dialogues and setting options. Not every task area has printer options available.

Page view

In this menu, you can specify which details and specifications you would like to print out. In the selection window that appears, you can highlight the elements to be printed and then by clicking **OK** go to the page view which then displays a preview of the print-out on the screen.

> ? Depending on the selected ***field of activity***, you have various selection dialogues and setting options. Not every task area has printer options available.

Print

Use this function to start the print procedure for the client settings or reports. In the selection screen that appears, you can specify which details and areas of the client settings you would like to print.

> ? Depending on the selected ***field of activity***, you have various selection dialogues and setting options. Not every task area has printer options available.

End

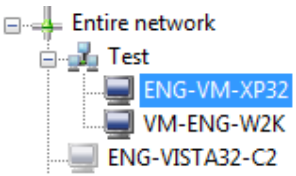
Terminate administrator use using this function. Naturally, the monitoring of your network continues to run uninterrupted according to the specifications that you transmitted to the ManagementServer when the administrator is not open.

Clients

In the clients menu, you can carry out basic settings for the work with the clients and groups that are to be administered.

New group

Use this command to create a ***group***. In principle this is a folder at the network level in which you can link and edit different clients together. When this command is enabled a new folder icon appears beneath the folder where the client selection area is located, where you can directly enter a new name for this group.



? In order to assign individual clients to this group as simply as possible, you can just use the mouse to drag them to the group entry. These clients then become sub-elements of the respective group.

Edit group

Here you can open a dialogue box where there are **Add** and **Remove** buttons you can use to group clients with one another. If you have not selected a group in the group selection area, this function cannot be selected.

? In order to assign individual clients to this group as simply as possible, you can just use the mouse to drag them to the group entry. These clients then become sub-elements of the respective group.

Delete

You can remove a computer from the list of clients to be monitored (***disable***) by highlighting it and selecting the **Delete** command from the client menu. Note that disabling a computer does not mean that the client software is uninstalled. Groups can only be deleted if the group is empty. Therefore you must either disable all clients in the group or move them to other groups. You can view deleted clients again via the **Display disabled clients** function.

Default settings

For the protection of the entire network or selected groups, you can create default settings and thereby quickly issue standardised specifications for virus protection. Thus, for example, you can simply move new clients into a group and automatically adopt the settings of the group for these clients.

? The default settings are only then available to you in the client selection area if you selected a group or the entry ***Entire network***. New clients that are integrated into the group assume the default settings and can be specified later if necessary.

? What relevance the individual settings and functions have on the default settings can be read in the section **Settings**

Delete default settings

The default settings of a group can be deleted via this function. In this manner, the default settings for the entire network are automatically transferred to the respective group.

Update view

To track changes in the network that occur during the time you are using the administrator, you can use the **Update** function.

Display disabled clients

Clients that you have not ***activated*** or have removed from the list of activated clients via the **Delete** function can be made visible again via this function. In doing so, ***disabled clients*** are shown as translucent icons.

In contrast to this, the ***activated clients*** are defined by fully coloured icons.

Activate client

If you select a disabled *G Data AntiVirus Client* (represented by a translucent icon) and click **Activate clients**, it will be activated.

In other words, it will be available to you for monitoring. No virus check is associated with it yet. You must create specifications for this in the task area **Monitor** or **Jobs** or assign the client to a group for which such specifications already exist. As soon as you install the *G Data AntiVirus client* on the *monitored* client computer, the virus protection is at your disposal.

Activate client (dialogue)

You can also ***Activate clients*** via this function without selecting them in the client selection area. By activating this function, a dialogue box appears in which you simply enter the name of the client that is to be activated.

Search for computer

By means of this function, you can search for computers within a defined range of ***IP addresses*** on your network. Simply enter the **Start IP address** and the **End IP address**. *G Data AntiVirus* now automatically searches through your ***host IDs*** for connected computers. You then have the option of activating the computers that were found. On one hand, you have the option of activating these via your computer names or directly addressing them via the IP address. The respective client then appears with his IP address in the client selection area.

Create AntiVirus Client installation packet

This function can be used to enable an installation packet for the *G Data AntiVirus Client* to be created. The packet is an individually executable file (***AvkClientSetupPck.exe***) with which a new client can be installed on a computer to protect it without any further user interaction being needed. The installation packet, for example, is capable of allocating the client to all computers in a domain via a login script.

? The packet always contains the current client version on the server.

View

You can use this menu to define the various software selection areas. The areas displayed are marked with a check. You can use the **Update** menu item to update the program interface at any time, for example, to take account of current view changes. You can find information on the areas in the relevant sections of the ***Task areas***.

Settings

In the settings menu you have access to basic program settings.

Internet update

You can run Internet updates for the virus database and *G Data AntiVirus* program files from here. First go to the **Login data and settings** tab to enter the login data you were given during ***online registration***. During the Internet update current files are loaded from the *G Data UpdateServer* and saved on the ManagementServer. Distribution of the new files to the clients is managed from the **Clients** task area. The Internet update ensures that you always have the most up-to-date virus signature databases and are using the most recent program files.

Virus database

All clients have a copy of the virus database so that virus protection is also guaranteed when they are offline (i.e. no connection to the ManagementServer is available). For example, this is important for ***notebooks***, which are only irregularly connected to their company network. ***Updating*** the files on the clients takes place in two steps, which, of course, can both be automated. In the first step, the latest files from the *G Data UpdateServer* are copied to a folder on the ManagementServer. In the second step, the new files are distributed to the clients (see task area " Clients").

- **Update status**: By clicking this button, you can, if necessary, update the virus signature status display on the client, if changes in the display have not yet been adopted.
- **Start update now**: By clicking the button **Start update now** you can carry out an immediate update of the virus database.
- **Automatic updates**: As with the virus checks, you can also let the Internet updates run automatically. To do this check the checkbox next to **Carry out periodic update** and specify when and with what cycle the update is to be carried out.

? To enable automatic updating, your ManagementServer must of course be connected to the Internet or enable *G Data AntiVirus* to carry out an automatic dial-up. To do this, under **Login data and settings** as necessary, enter the ***user account*** and ***proxy settings***.

Program files

When the ***client software*** from ***G Data*** is updated, you can allow the ManagementServer to carry out the update automatically. ***Updating*** of the files on the clients takes place in two steps, which, of course, can both be automated. In the first step, the latest files from the *G Data UpdateServer* are copied to a folder on the ManagementServer. In the second step, the new files are distributed to the clients where the client is updated (see ***Clients task area***).

- **Update**: By clicking the **Update** button, you can, if necessary, update the software version status display on the client, if changes in the display have not yet been adopted.
- **Update now**: By clicking the button **Update now** you can carry out an immediate update of the client software.

- **Automatic updates**: As for the virus checks, you also let the client software Internet updates run automatically. To do this check the checkbox next to **Carry out periodic update** and specify when and with what cycle the update is to be carried out.

? To enable automatic updating, your ManagementServer must of course be connected to the Internet or enable *G Data AntiVirus* to carry out an automatic dial-up. To do this, under **Login data and settings** as necessary, enter the ***user account*** and ***proxy settings***.

? ***Warning***: To update the ManagementServer program files, please select program group ***G Data AntiVirus ManagementServer*** then select the entry ***Internet update*** from the start menu. The ManagementServer may only be updated via this entry. By contrast, *G Data AntiVirus client software*, can also be updated via the administrator.

Login data and settings

With your ***online registration*** you will receive your login data for updating your virus databases and program files directly from ***G Data***. Please enter the necessary data under **User name** and **password**. Via the button **Version check** you can determine at the next update of the virus database whether you are using the latest program files. In general version check should always be switched on, because it prevents unnecessary updates. Nevertheless, should problems occur when working with virus databases, then please switch the field **Version check** off. In this way, at the next Internet update, a current version of the virus database will be transferred to your server. By clicking the button **User account and proxy settings** you open a window in which basic login data for the Internet & Network can be entered.

? ***Warning***: You should only make entries here if problems occur when using the standard settings of *G Data AntiVirus* (e.g. due to the use of a ***proxy server***) and an Internet update is not executable.

Internet settings

Required for the user account is the information: **user name**, **password** and **domain**. For logging on to the ***proxy server***, the port (usually 80) and - if different from the user account - entry of the user name and password for the proxy server are required.

? **User account** is an account for the computer on which the ManagementServer is located, i.e., for Windows Vista or Windows XP professional, whichever is installed on it.

? *G Data AntiVirus* can use the ***Internet Explorer connection data*** (from version 4). First configure ***Internet Explorer*** and check whether the test page of our update server is accessible: ***http://ieupdate.gdata.de/test.htm***. Finally switch off the option **use proxy server**. Under **User account** enter the account for which you have configured Internet Explorer (as the account with which you have logged in to your computer).

Alarm notifications

If a new virus is found, the ManagementServer can automatically send alarm notifications via ***email***. The settings required to do this are made here.

Email settings

Enter the name of your network mail server, **SMTP server** and the **port** (normally 25). In addition a (valid) sender address is required so mails can be sent.

? This email address will also be used for responses from the ***Emergency AntiVirus service*** .

Email notification

Activate email notification by checking the **Send alarm notifications by email** checkbox and entering the email address for the notification recipient in **Recipient**. It is essential to define a quantity limit under **Limit** so the mailbox is not filled to capacity during acute attacks.

Update rollback engine A / B

Where a false alarm or similar problems occur, it can, in rare cases, make sense, to block the latest ***update of the virus signatures*** and use a previous virus signature update instead. The ManagementServer saves the last updates from each AntiVirus engine. Should the latest update for engine A or B result in problems, the administrator can block the latest update for a certain time interval and instead of this distribute a prior signature update to the clients and subnet servers.

? On clients that are not connected to the ManagementServer (e.g. notebooks used in business travel), no ***rollbacks*** can be carried out. Here a block transferred from the server to the client cannot be applied retroactively.

? The number of rollbacks to be saved can be specified in the area **Server settings** .

Server settings

Here you can make the basic settings for synchronisations and automatic delete procedures.

Settings

You will find the following options in the settings area:

- **Rollbacks**: Indicate here how many of the updated virus signature updates you would like to hold as a reserve for ***Rollbacks***. The default value here is the last 10 signature updates for each engine.
- **Automatically clean**: Here you can define that: ***log entries***, ***scan logs*** and ***reports*** are automatically deleted after a specified period of time.

Synchronisation

In the synchronisation area you can schedule communication between clients, subnet servers and servers:

- **Clients**: Here you enter the time interval in which the clients are synchronised with the server. If you set the check next to **Notify clients of option changes from the server**, then the user receives a message on the client computer that changes have been carried out.

- **Subnet server**: in this area you can define the intervals for communication between server and subnet server. If you set the check next to **Transfer new reports to the main server immediately**, the reports will be transferred to the main server immediately, independently of the settings made here.

Help

Here you can access information on the program and also have the option of accessing the online help function of *G Data AntiVirus*. Use the **online virus encyclopaedia** function to access the *G Data virus encyclopaedia*. This gives you an interesting insight into the far-reaching world of viruses and malware. As the virus encyclopaedia is constantly being updated, you can find it on the Internet as an online encyclopaedia. Clicking on this text will set up an Internet connection. If there is no Internet connection available, the virus encyclopaedia cannot be displayed.

? Viewing information in the ***virus encyclopaedia*** at ***www.antiviruslab.com*** is of course free of charge - apart from the ISP-related fees that you pay for your Internet connection.

Toolbar

In the toolbar you will see the most important commands from the ***Menu bar*** displayed as clickable icons.

New group: The activated computers can be linked into ***groups***. Easily distinguishable security zones can be defined since all settings can be made for both single clients and for entire groups. To create a new group first highlight the superordinate group then click on on the icon displayed.

Delete: You can remove a computer from the list (***disable***), by highlighting it and then clicking on the **Delete** button. Note that disabling a computer does not mean that the client software is uninstalled.

Update view: Use **Update** or the ***F5*** key to update the appearance of the Administrator interface at any time, for example to take account of current changes to the display.

Display disabled clients: Select this button to display disabled computers as well. You can recognise the disabled computers by their greyed-out icons. Computers without file sharing or printer sharing are not normally shown.

Activate client: To activate a computer, highlight it in the list and select the button displayed. You can also activate computers that do not appear in the list. To do this, in the client menu select the **Activate client (dialogue)** command and enter the computer's name.

Display log: The log file gives you a fast, global overview of *G Data AntiVirus*'s last actions. All relevant information is displayed here.

Internet update: You can use the ***Internet update*** area to run Internet updates for the virus databases and the client program files.

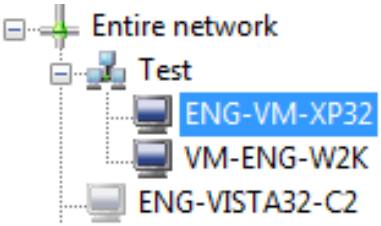
Alarm notifications: If a new virus is found, the ManagementServer can automatically send alarm notifications via email. The settings required for this can be found in the **Alarm notifications** area in the **Settings** menu.

Online virus encyclopaedia: Use the **Online virus encyclopaedia** function to access the*G Data AntiVirus virus encyclopaedia*. This gives you an interesting insight into the far-reaching world of viruses and malware. As the ***virus encyclopaedia*** is constantly being updated, you can find it on the Internet as an online encyclopaedia.

Help: With this button you can fall back on the online help of *G Data AntiVirus*.

Client selection area

Here you will find all clients and servers as well as defined groups in your network listed hierarchically and subdivided. As in Windows Explorer, groups that have subdivisions appear with a plus symbol. If you click this, the directory structure opens up here and enables the view of the structure behind it.



Clicking the minus symbol closes the subdivision again. The following icons are visible in the Directory selection:

Network icon

Group

Server (activated)

Server (disabled)

Client (activated)

Client (disabled)

Non-selectable devices: For example, network printers fall under this category

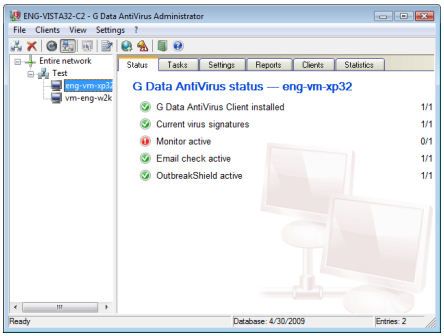
Task areas

You have the opportunity to conveniently administer the protection of your clients in the different task areas that you can select via the respective tabs. The settings you enter here always relate to the clients or groups that you have highlighted or selected in the ***Client selection area***. The different subject fields are explained in detail in the sections below.

- **Status**
- **Jobs**
- **Settings**
- **Reports**
- **Clients**
- **Statistics**

Status

In the Statusarea of *G Data AntiVirus* you receive basic information about the current state of your system. This information, consisting of text, figures or dates, is displayed to the right of each item.



As long as your system is optimally configured for protection from computer viruses, you will see a green traffic light icon to the left of the listed entries.

If a component is not optimally set (e.g. switched off monitor or obsolete virus signatures), a warning symbol will alert you.

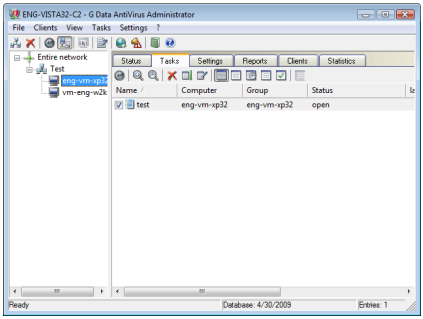
? When the *G Data AntiVirus program interface* opens, most of the icons will be displayed in warning mode for a short duration. This does not mean that *G Data AntiVirus* is not protecting your computer during this time; quite the opposite: an internal virus protection status check is underway, which indicates to you that automatic checking of the functions is underway.

By double-clicking the respective entry, you can undertake actions here directly or change to the respective function. Once you have optimised the settings for a component displaying a warning icon, the icon in the status area reverts to the green traffic light icon..

Jobs

In this task area you can define jobs for virus checks on the *G Data AntiVirus Clients*. There are two different job types: ***single scan jobs*** and ***periodic scan jobs***. Single scan jobs are performed immediately after they are created, for the periodic jobs a ***Schedule*** is defined according to which they are run.

? ***Scan jobs*** or ***jobs*** are the corresponding tasks that you create in the task area of the same name for virus checking, removal or prevention.



In the **jobs** task area all jobs appear under the name given to them by you and can be sorted according to the following criteria by simply clicking on the respective column designation. The column according to which current sorting is carried out, is indicated by a small arrow symbol:

- **Name**: The name specified by you for the scan job. You can enter a name of any length here and thereby precisely describe your scan job in order to maintain an overview when there are a large number of different jobs.

- **Computer**: You will find the name of the corresponding client here. You can only define scan jobs for activated clients.
- **Group**: You can combine individual clients into groups which then use the same scan jobs. If you assign a scan job to a group, the individual computers do not appear in the overview list but rather the group name.
- **Status**: Here you obtain the status or the results of a scan job displayed in clear text. Thus, for example, you see whether the job has just run or has been completed, and also whether or not viruses were found.
- **Last run**: Via this column, you receive information as to when the respective scan job was last run.
- **Time interval**: According to the ***Scheduling*** that you can define for every scan job, this states in which cycle the job will be repeated.
- **Analysis scope**: Here you find out to which ***data media*** (e.g. local hard disks) the analysis extends.

? In the menu bar, an additional menu entry with the following functions is available for the task area **jobs**:

- **View**: Select whether you would like to display all ***scan jobs***, only single scan jobs, only periodic scan jobs or only open scan jobs or only completed scan jobs here. For scan jobs that were defined for a ***group*** of clients, you can decide whether detailed information about all clients or only cross-group summaries should be displayed. Set the checkmark here next to **Display group jobs in detail**.
- **Run again (immediately)**: This enables you to run selected scan jobs independently of any scheduled jobs.
- **Cancel**: You can cancel a running scan job with this function.
- **Delete**: Selected scan jobs can be deleted using this function.
- **New**: Select whether you want to create a ***one-time scan job*** (single test) or a ***regular scan job*** (periodic test) here.

You can define as many different scan jobs as you would like. For performance reasons, it generally makes sense that scan jobs do not overlap.

Update

This function updates the view. Loads the current job list from the ManagementServer.

New scan job (single)

Use this function to set up a new job for single tests. It opens a dialogue for entering job and scan parameters. You can enter the settings you want here. When so doing you can change between settings areas by simply selecting the relevant tab. These tabs are explained in detail in the section **New scan job (periodic)**.

? You can use the **New scan job (periodic)** function to define scheduled scan jobs for automatically checking your system at regular intervals.

? Double-click to change the parameters for an available job in the list, or select the ***Properties*** command from the context menu (by right-clicking the mouse). You can now change the scan job settings to what you want.

New scan job (periodic)

Use this function to set up a new job for periodic scans. It opens a dialogue for entering job and scan parameters. You can enter the settings you want here. When so doing you can change between settings areas by simply selecting the relevant tab:

? Double-click on the entry to change the parameters for an available job, or select the ***Properties*** command from the context menu (by right-clicking the mouse). You can now change the scan job settings to what you want.

Job

Use the job parameters to define what name the scan job should have. For example, you can enter meaningful names here such as ***Archive scan*** or ***Monthly scan*** to unambiguously label the desired job so that it can be found again in the tabular overview. In addition you can also enter whether the user can cancel the job via the client context menu. If you use the monitor to permanently monitor your network, it is OK to let the scan job be cancelled by the user as it may have a slight impact on his working speed. However, if you do not use the monitor, periodic scans are absolutely indispensable and should not be able to be switched off. You can use the **Regularly transmit scan progress to the server** option to have the status of a scan process running on a client displayed as a percentage on the Administrator. The **Shut down computer after virus check if no user is logged on** function provides another way to help reduce your administrative load.

Time/scheduling

This tab allows you to specify when the automatic update should run and how often. You set up the default schedule under **Run** which you then specify with the entries under **time** and **weekdays**.

If you select **On system start** the scheduling defaults naturally no longer apply and *G Data AntiVirus* will run the update each time your computer is restarted.

? Under **daily** you can specify using the settings under **weekdays** to specify for example that the computer should only carry out the update on working days or even only every other day or on weekends only, when it is not being used for work.

Scanner

In the scanner menu, you can specify how the virus check is to be carried out by *G Data AntiVirus*.

As scheduled or manual analysis virus checks usually take place when the computer is not running at full load to perform other tasks, more system resources are usually available for virus analysis than for the ***Virus monitor***.

- **Use engines**: *G Data AntiVirus* uses two antivirus engines; essentially two, independently operating virus analysis units. In principle, you must

use both engines to guarantee optimum virus prevention results. However, using a single engine does have performance benefits – analysis can be performed more quickly if only one engine is used. We recommend the setting **Both engines - performance optimised**. In this scenario, both virus scanners cooperate such that optimised detection accuracy is achieved within a minimised scanning duration.

- **In case of an infection**: Here you can specify the action to be taken if an infected file is detected. There are various options here that may or may not be suitable, depending on what purposes the client is used for. The setting **Move file to quarantine** is a special directory which the ManagementServer creates and in which infected files are encrypted and thus can be stored without having any continuing harmful effect. Files in ***quarantine*** can be disinfected by the administrator, deleted, moved back to their original storage location or, if required, sent to the ***Emergency AntiVirus service*** of ***G Data***.

- **Infected archive**: Specify here whether the processing of virusses found should be carried out differently for ***archives***. In this respect you should bear in mind that a virus in an archive will only be harmful, when it is unpacked from the archive.

- **File types**: Here you can define the file types *G Data AntiVirus* should check for viruses. Generally it is not necessary to check files that do not contain any executable program code, on top of which checking of all the files on a computer requires a not inconsiderable amount of time. We recommend **automatic type recognition** with which only those files which could theoretically contain a virus are checked.

- **Priority scanner**: You can use the levels ***high***, ***medium*** and ***low*** to specify whether virus checking by *G Data AntiVirus* should have high priority on your computer (in which case the analysis is relatively quick and other applications may run more slowly during the analysis) or low priority (the analysis runs relatively slowly, so that other applications can continue to run relatively unaffected during this period). Depending on the time you take to run the virus analysis, different settings are useful here.

- **Settings**: Specify the additional virus analyses you want *G Data AntiVirus* to perform. The options selected here are generally recommended. Depending on the type of application, the time gained by omitting these checks may outweigh the slightly reduced level of security. The following configuration options are available:

Heuristics: Heuristic analysis detects viruses not only on the basis of constantly updated virus databases, but also based on detecting characteristics that are typical of most viruses. The heuristics can generate a false alarm in rare instances.

Archives: Checking of compressed data contained in archives is very time consuming and can generally be suppressed if the ***G Data AntiVirus monitor*** is active on the system. The monitor can detect a previously hidden virus while the archive is being unzipped and can automatically prevent it from spreading. Nevertheless, during regular checks of the computer outside the actual usage times, checking of the archives should also take place.

Email archives: Checking of compressed data contained in email archives is very time consuming and can generally be suppressed if the ***G Data AntiVirus monitor*** is active on the system. The monitor can detect a previously hidden virus while the archive is being unzipped and can automatically prevent it from spreading. Nevertheless, during regular checks of the computer outside the actual usage times, checking of the archives should also take place.

System areas: The system areas of your computer ***boot sectors***, ***master boot records*** etc.) which form the essential foundation of the operating system, should generally not be excluded from virus checking.

Check for diallers / spyware / adware / riskware: With *G Data AntiVirus* you can also check your system for ***diallers*** and other malware (***spyware***, ***adware***, ***riskware***). These are e.g. programs that establish expensive, unwanted Internet connections, of which the potential for financial damage is no less significant than that of the virus. They may for example secretly record your surfing habits or even all the keyboard entries you make (including your passwords) and forward these to third parties via the Internet at the earliest opportunity.

Use all available processors: With this option, you can distribute the virus checking load on systems with multiple ***processors*** (e.g. DualCore), over all the processors with the result that the virus checking runs considerably quicker. The disadvantage of this option is that the system speed for other applications is considerably reduced. Thus you should only use this option, if you are running your scan job at times, when the system is not normally used (e.g. overnight).

Analysis scope

You can also limit the virus control on the client to specific directories via the tab **Analysis scope**. In this way for example, you can omit folders with archives that are seldom used or integrate them in a special scan schedule. When so doing, the Directory selection refers to the currently selected computer and not to the selected client.

? ***Special feature for scan jobs on a Linux file server***: The root drive (/) and all authorisations will be returned with the directory selection. Scan jobs can thus be performed in a targeted manner based on selected authorisations or on file server directories selected as desired.

Delete scan jobs

The function **Delete scan jobs** deletes all highlighted jobs.

Run scan jobs again (immediately)

Select this function, to re-run one-off scan jobs, which have already been run or cancelled. For periodically executing scan jobs, this function causes the job to be run independently of the schedule.

Logs

Use this function to call up the logs relating to a particular client's jobs.

Show options

With a large number of different scan jobs, it is useful to show and list these according to particular criteria. The following options are available:

Show all jobs

Only show single scan jobs

Only show periodic scan jobs

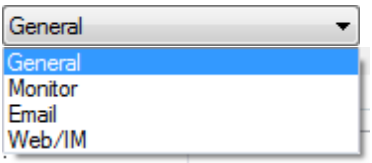
Only show open scan jobs

Only show completed scan jobs

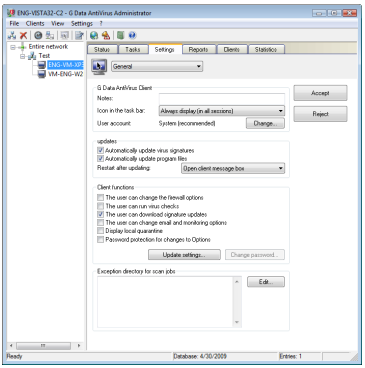
Display group jobs in detail: Displays all associated entries with group jobs. The option is only available if a group is selected in the computer list.

Settings

Options for all clients, individual clients or a group of clients can be set in this task area (e.g. whether updates should be performed automatically, whether internal Internet updates via the clients are permitted, whether exception directories are allowed to be individually defined there, etc.).



Via the selection box found above, you can decide which type of options you would like to edit here. In the ***Client selection area*** select the desired client for this or the group of clients that you would like to configure, then execute the desired entries and close the procedure by clicking the **Accept** button.



General

Here, you have the following setting options:

G Data AntiVirus Client

The following functions are available:

- **Comment**: Enter a distinctive name for the relevant client
- **Symbol in the taskbar**: For terminal servers and Windows XP or Vista with fast user switchover you can select the sessions in which a client symbol should be displayed in the taskbar: ***never***, ***only in the first session*** or ***always***. For *normal* clients, the client symbol can optionally be prevented from being displayed. The symbol must be displayed to allow the user to access advanced client functions, because access to the relevant ***Context menu*** is enabled from this via a mouse click.
- **User account**: The client software normally runs in a system environment (Windows 2000 / Windows XP / Windows Vista / Windows 2003). You can enter another account here to enable network directories to be scanned. To do this, the account must have administrator rights for the client.

Updates

The following functions are available:

- **Update virus signatures automatically**: Switches on the automatic update of the virus database. Clients periodically check whether a new version is available on the ManagementServer and execute an automatic update.
- **Automatically update program files**: Updates the program files on the client with the files held on the ManagementServer. A client reboot may be necessary after updating the program files. Dependent on the setting under **Restart after update** the client user has the option of shifting the data update to a later point in time.
- **Restart after update**: You can specify here whether the client is automatically restarted after the program files are updated (**Restart without querying**), whether the user is offered the option to carry out a restart immediately or later (**Open client display window**) or whether the update of the program files is only carried out when the client is rebooted next (**Create report**).

Client functions

With the following functions, you defined the appearance, behaviour and functional scope of the respective client. Depending on the procedure, the user thus has extensive or only strongly limited rights with regard to virus prevention and countermeasures.

- **The user can run virus checks**: In an acute suspicious case, the user can run a ***virus check*** on his computer as he would with a locally installed antivirus solution independently from the ManagementServer. Results of this virus check will be transmitted to the ManagementServer during the next contact with it.

- **The user can download signature updates**: If you enable this function, the respective client can download virus signatures directly from the Internet even without connection to the company server. This significantly increases security for notebooks used by field service staff.

- **The user can change email and monitoring options**: If this function is enabled, the client user has the option, in addition to the ***monitor options*** , of influencing the settings in a targeted way where ***email security*** for his client is concerned.

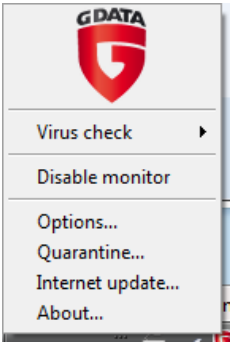
- **Display local quarantine**: If you allow the display of the local ***quarantine*** , the user can, if necessary, disinfect, delete or move back data that was moved by the monitor into this Quarantine folder due to virus infection or suspicion. Note that the virus would not be removed during a move back. You should therefore only enable this option for experienced users on the client.

- **Password protection for changes to options**: If the right to change the monitor options was granted to the user on the clients, the possibility naturally always exists that other people on this computer improperly switch off the monitor functions. To prevent this, you can protect the monitor option settings on the client with a password. Individually assign the password here for the respective client or the respective group and disclose it only to the authorised users of the client computer.

- **Update settings**: Here you can specify whether the Internet update of virus signatures should occur generally via the server, individually for every client, or a combination of the two. It is precisely with mobile workplaces that are only occasionally connected to the company network that a combination of the variants is recommended. Via the **Settings and scheduling** button you can additionally define individual reference settings

for the virus signatures for this client.

The following context menu is made available on the client computer to a client activated with full user rights:



Exception directories for scan jobs

You can define client directory exceptions here that are not to be checked during the execution of scan jobs. Archive and backup areas of a hard disk or partition, for example, can be defined as exception directories where applicable.

? Exception directories can be defined for complete ***groups***. If the clients in a group have defined different exception directories, new directories can be added or existing ones can be deleted. The directories specially defined for individual clients are thereby preserved. The same procedure is also used with the monitor exceptions.

? ***Special feature on a Linux file server***

The root drive (/) and all authorisations will be returned with the exception directories selection. In doing so, drive exceptions, directory exceptions, and file masks can be created.

Monitor

The monitor settings in the ***Client selection area*** for the selected client can be made here. Select a group to change the monitor settings of all clients in the group. You can adjust individual settings in the **Monitor** area for every client/group. The changed settings are only saved and set by the clients after pressing the **Accept** button. Press the **Reject** button to load the current settings from the ManagementServer without accepting the changes.

> **?** If you edit the monitor setting of a ***group***, the individual parameters can adopt an undefined status. In this case, the clients of the group have different settings for the parameter. Undefined parameters are not saved during the transfer.

First and foremost, you should never switch off the monitor on the clients without a good reason because it significantly contributes to the data security of your network. As soon as you have activated the monitor on a client, it always remains active in the background automatically.

> **?** There can be considerable delays when using certain programs or components (e.g. ***T-Online***, ***Microsoft Office*** with certain ***HP printers***). To avoid this, you can define the INI files for these products as exceptions. This significantly shortens the checking process but also presents a certain security risk. This must be weighed.

Settings

The following functions are available in the settings area:

- **Monitor status**: From here you can switch the monitor on and off. In general you should leave the monitor switched on. It forms the foundation for permanent and uninterrupted virus protection.
- **Use engines**: *G Data AntiVirus* works with two independently-operating virus analysis units. In principle, using both engines guarantees optimum results for preventing viruses. On the other hand, using just one engine has certain performance advantages.
- **In case of an infection**: Here you can specify the action to be taken if an infected file is detected. There are various options here that may or may not be suitable, depending on what the respective client is used for.

Block file access: Neither read nor write access can be granted for an infected file.

Disinfect (if not possible: block access): An attempt is made to remove the virus; if this is not possible, file access is blocked.

Disinfect (if not possible: place in quarantine): An attempt is made to remove the virus; if this is not possible, the file is moved to ***Quarantine*** .

Disinfect (if not possible: delete file): An attempt is made to remove the virus; if this is not possible, the file is deleted.

Move file to quarantine: The infected file is moved to quarantine. The system administrator can be used to try to manually run a disinfection on the file.

Delete infected file: This function serves as a strict measure for effectively containing a virus. Depending on the virus however, it can cause considerable data loss.

- **Infected archive**: Define here if viruses found in archives should be handled differently. In this respect you should bear in mind that a virus in an archive will only be harmful, when it is unpacked from the archive.

- **File types**: Here you can define the file types *G Data AntiVirus* should check for viruses. Generally it is not necessary to check files that do not contain any executable program code, on top of which checking of all the files on a computer requires a not inconsiderable amount of time. We recommend the **Automatic type recognition** here with which only those files are automatically checked which could theoretically contain a virus.

- **Check when writing**: Normally a virus-free system does not generate files infected with viruses when writing files; however, in order to cover all eventualities, particularly with systems in which a ***Bootscan*** was not run, you can set up a scan procedure here for use when writing files. The huge advantage of this is that even viruses which are copied from another possibly unprotected client to an enabled directory of the client protected by the monitor are detected and that files downloaded from the Internet are first recognised as virus-afflicted during loading and not during first execution.

- **Check network access**: Here you can specify operation of the monitor in conjunction with network access. If your entire network is normally monitored by *G Data AntiVirus*, network access verification may be discontinued.

- **Heuristics**: In a heuristic analysis, viruses are not only detected using the constantly updated virus databases but also using certain traits characteristic of viruses. On the one hand, this method is an additional security benefit; on the other, it can also give rise to a ***false alarm*** in rare cases.

- **Check archive**: Checking compressed data in archives is a very time-consuming process and can generally be omitted if the *G Data AntiVirus virus monitor* is always enabled on your system. The monitor can detect a previously hidden virus while the archive is being unzipped and can automatically prevent it from spreading. To avoid decreasing performance with unnecessary checks of large archive files that are rarely used, you can set a size limit (number of kilobytes) for archives to be checked.

- **Check email archives**: This option should generally be disabled as scanning email archives generally takes a long time and if an infected mail is found it is impossible to read further mails. As the monitor blocks execution of email attachments, disabling this option does not create a security hole. When using ***Outlook***, incoming and outgoing mails are also scanned using an integrated plug-in.

- **Check system areas on system start-up**: In general, system areas (for example ***boot sectors***) in your computer should not be excluded from virus checks. You can specify here whether you want to check them on system start-up or whenever media are changed (insertion of a new CD-ROM etc). Generally you should have at least one of these two functions activated.

- **Check system areas on media exchange**: In general, system areas (for example ***boot sectors***) in your computer should not be excluded from virus checks. You can specify here whether these should be checked on system start-up or whenever a ***media change*** occurs (new CD-ROM etc.). Generally you should have at least one of these two functions activated.

- **Check for diallers / spyware / adware / riskware**: With *G Data AntiVirus* you can also check your system for ***diallers*** and other malware (***spyware***, ***adware***, ***riskware***). These are e.g. programs that establish expensive, unwanted Internet connections, of which the potential for financial damage is no less significant than that of the virus. They may for example secretly record your surfing habits or even all the keyboard entries you make (including your passwords) and forward these to third parties via the Internet at the earliest opportunity.

Exceptions

Here you can also limit client virus checking for specified directories. In this way for example, you can omit folders with archives that are seldom used or integrate them in a special scan schedule. Furthermore, certain files and file types can be excluded from the virus check. The following exceptions are possible:

- **Drive**: By clicking the directory button here, you select a drive (***partition***, ***hard disk***) that you do not want checked by the monitor.
- **Directory**: By clicking the directory button here, you select a ***folder*** (as necessary, including any ***subfolder*** contained within it) that you do not want checked by the monitor.
- **File**: Here you can enter the name of the file that you would like excluded by the monitor check. You can also use wildcards here (e.g. the question mark (?) for any single character or the asterisk (*) for any number of characters).

You can repeat this procedure as many times as you wish, and you can delete or modify the existing exceptions in the **Monitor exceptions** window.

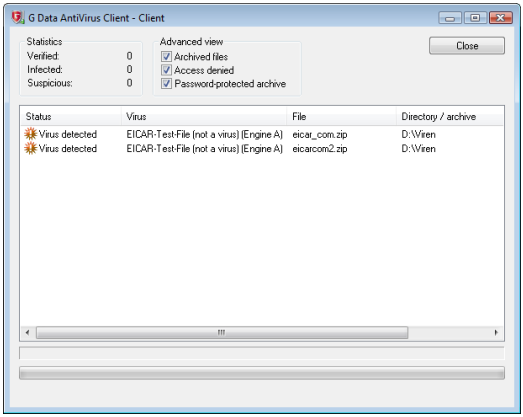
? ***Wildcards*** work as follows:

- The ***question mark symbol*** (?) represents individual characters.
- The ***asterisk symbol*** (*) represents entire character strings.

For instance, in order to protect all files with the file extension ***exe***, enter ****.exe***. For example, to protect files with different spreadsheet formats (e.g. ***.xlr***, ***.xls***), simply enter ****.xl?***. Or to protect files of various types that have identical initial file names, enter e.g. ***text*.****.

Warning messages

Specify here whether the user on a client computer is notified when a Virus found event occurs. If the checkmark is set here, the user sees an info window that informs him of the viruses found.



Status

Here you are shown whether the changes you have made to the monitor have already been transferred to the client or the group or whether you have not yet clicked the **Accept** button.

Email

Special virus protection can be set up on every *G Data AntiVirus client* especially for email. The protocols ***POP3***, ***IMAP*** and ***SMTP*** are checked in the ***TCP/IP layer*** here. Furthermore, a special ***plug-in*** is used for ***Microsoft Outlook***. The plug-in automatically checks all incoming mails for viruses and prevents infected mails from being sent. By clicking the **Accept** button, you accept the executed changes; by clicking **Cancel**, you exit the dialogue without accepting the executed changes. You can create individual configurations for handling mail for every client or for user groups via the administrator. In this respect, you can select from the following options:

Incoming mails

The following functions are available:

- **In case of an infection**: Here you can specify the action to be taken if an infected file is detected. There are various options here that may or may not be suitable, depending on what the respective client is used for.

- **Check received mails for viruses**: By enabling this option, all emails that the client receives online will be checked for viruses.

- **Check unread mails on program start-up (Microsoft Outlook only)**: This option is used to scan emails for viruses that the client receives while it is offline. AntiVirus will check all unread mails in your Inbox folder and subfolders as soon as you open ***Outlook***.

- **Append report to received, infected mails**: As soon as one of the emails sent to the client contains a virus, you will receive the following message in the body of this mail beneath the actual mail text: ***WARNING! This mail contains the following virus*** followed by the name of the virus. In addition, you will find the notification ***VIRUS*** before the actual subject. If you enabled the option **Delete attachment/text**, you will also be notified that the infected part of the email was deleted.

Outgoing emails

The following functions are available:

- **Check emails before sending**: So that you do not unintentionally send viruses from your own network, *G Data AntiVirus* also offers the possibility of checking outgoing emails for viruses before sending them. If a virus actually does get sent, the message ***The mail [subject header] contains the following virus: [virus name]*** appears. The mail cannot be sent, and the corresponding email will not be sent.

- **Append report to outgoing email**: A certification report is displayed in the body of each outgoing email below the actual mail text. This reads ***Virus checked by G Data AntiVirus***, provided that you have enabled the option **Check mails before sending**. Additionally, you can specify the version date of *G Data AntiVirus* (**Version information**) and a link to the ***G Data virus encyclopaedia*** (**Virus News**) here.

Scan options

The following functions are available:

- **Use engines**: *G Data AntiVirus* uses two antivirus engines; essentially two, independently operating, virus analysis units. In principle, you must use both engines to guarantee optimum virus prevention results. However, using a single engine does have performance benefits – analysis can be performed more quickly if only one engine is used.

- **OutbreakShield**: OutbreakShield detects and neutralises threats from malware in mass mailings before the relevant up-to-date virus signatures become available. The OutbreakShield uses the Internet to monitor increased volumes of suspicious emails, enabling it to eliminate the window between the mass mailing outbreak and the application of designated virus signatures to contain it, practically in real time. Under **change** you can specify whether OutbreakShield uses additional signatures to increase detection performance. Loading of the signatures may cause automatic Internet connections to be made. In addition you can also enter access data here for the Internet connection, which then permits OutbreakShield to carry out an automatic signature download from the Internet.

Warning messages

Inform user when a virus is found: You can inform the recipient of an infected email automatically of this event. Accordingly a warning message is displayed on his/her desktop.

Email protection

The following functions are available:

- **Protect Microsoft Outlook through an integrated plug-in**: Activation of this function inserts a new function in the ***Outlook*** program of the client under the ***Tools*** menu, called ***Check folder for viruses***. Independent of the administrator settings, an individual client user can scan the currently selected email folder for viruses. In the email display window you can use ***Scan mail for viruses*** in the ***Tools*** menu to run a virus check of the file attachments. When the process has been completed, an information screen appears in which the result of the virus check is summarised. Here you can see whether the virus analysis was completed successfully, get

information about the number of emails and attachments scanned and about any read errors, as well as any viruses found and how they were dealt with. You can hide both windows by clicking on the ***Close*** button.

- **Monitor ports**: Generally speaking, the ***default ports*** for ***POP3***, ***IMAP*** and ***SMTP*** are monitored. If your system's port settings are different than these, you can customise this accordingly.

Web / IM

You can undertake the following settings here.

Internet content (HTTP)

- **Process Internet content (HTTP)**: In the web options, you can determine that all ***HTTP web content*** is checked for viruses whilst browsing. Infected web content is not run at all and the corresponding pages are not displayed. To set this option, please check **Process Internet content (HTTP)**.

- **Avoid browser timeout**: Since *G Data software* processes web content before it is displayed in the Internet browser, it requires a certain amount of time to do so depending on the data traffic. Therefore it is possible for an error message to appear in the Internet browser because the browser does not receive data immediately, due to the antivirus software checking it for malicious routines. By activating the checkbox **Avoid browser timeout**, you can disable this error message and as soon as all browser data has been checked for viruses, the data will appear as normal in the Internet browser.

- **Download size limit**: With this function you can interrupt the HTTP check for web content that is too large. The contents are then monitored by the virus monitor as soon as suspected malicious routines become active. The advantage of the size limit is that there are no delays caused by virus checks when surfing the web.

Instant Messaging

- **Process IM content**: Since viruses and other malware can also be spread via Instant Messaging, *G Data software* can also prevent infected data from being displayed and downloaded in advance. If your Instant Messaging applications do not run using standard port numbers, please enter the corresponding ***port addresses*** under Server port number(s).

- **Instant Messaging (integration into IM application)**: If you use ***Microsoft Messenger (version 4.7 and later)*** or ***Trillian (version 3.0 and later)***, you can set the checkmark for the respective program to define a context menu in which you can directly check suspicious files for viruses.

> **?** If you do not want to check the Internet content, the **Virus monitor** naturally takes action if infected files are started. That means that the system on the respective client is also protected without checking Internet content as long as the virus monitor is active.

AntiSpam

You can undertake the following settings here.

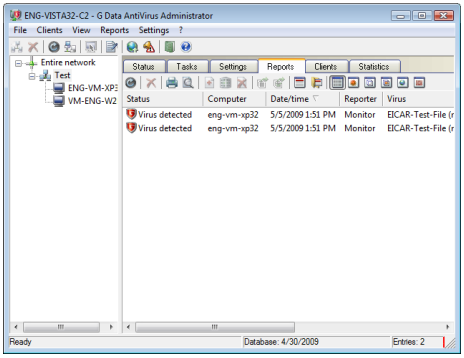
Spam filter

If you set the checkmark next to **Use spam filter** client email traffic will be checked for possible spam mails. As soon as an email is identified as spam or falls under suspicion of being spam, you can define a warning that will be displayed in the subject line of the email.

> **?** You or the user can define a rule on the client in the mail program where, for example, mail that has ***[Spam]*** in the subject line will automatically be moved to the recycle bin or a special folder for spam and junk mail.

Reports

All virus results will be displayed in this task area. The status of the report will be displayed in the first column of the list (e.g. ***Virus detected*** or ***File quarantined***). If a virus is found, you can respond by selecting the entries in the list and subsequently selecting a command from the context menu (right mouse button) or from the toolbar. Thus, for example, infected files can be deleted or moved in the ***Quarantine folder*** .



In the **reports** task area all reports appear under the name given to them and can be sorted according to different criteria by simply clicking on the respective column name. The column according to which current sorting is carried out, is indicated by a small arrow symbol.

The following criteria are available:

- **Status**: You receive a short and concise display of the content of the respective report here. Informative icons underscore the importance and type of the respective report.
- **Computer**: The computer from which the respective report is made is displayed here. All computers are listed individually with user groups.
- **Date/time**: The date on which the report is created, based either on an acute virus result through the *G Data AntiVirus monitor* or on the basis of a scan job.
- **Reporter**: Through this entry, you are informed whether the report arises from the ***virus scanner*** as the result of a scan job, automatically through the ***monitor***, or via the *G Data AntiVirus mail plug-in*.
- **Virus**: if known, the name of the virus detected is displayed here.
- **File / mail**: The file in which a virus is found or in which a suspected virus exists is listed here. For ***email***, you will also find the email address of the sender listed here.

- **Folder**: Directory information for the file concerned is important in case a file is quarantined and is subsequently to be moved back again.

? In the menu bar, an additional menu entry is available for the task area **reports**. For functions that operate with files (delete, move back, etc.), you must select the respective file or files in the report overview. You can select the following functions here.

- **View**: Indicate whether you would like to see all reports, only reports with viruses not removed or only quarantine reports here. You can also view the quarantine content.
- **Hide dependent reports**: If, due to different jobs or jobs that were performed multiple times, a virus alert or a report is displayed twice or more, you can hide the duplicate using this option. Only the most current entry is then shown and can be edited.
- **Hide archived files**: Here you can hide or show messages about reports from archive checks. If a virus is found in an archive, *G Data AntiVirus* generally issues two messages in which the first message shows that an archive is infected and the second message shows precisely which file in THIS archive is affected. If you use the function **Hide archived files**, both of these messages are combined.

If you have set up the ***scanjobs*** on your system so that these simply log viruses found, you can also execute the virus countermeasures manually. To do this, select one or more logged file(s) in the report and then run the desired operation:

- **Remove virus from the file**: Attempts to remove the virus from the original file.
- **Move file to quarantine**: Moves the file to the ***quarantine*** folder.
- **Delete file**: Deletes the original file on the client.
- **Quarantine: Clean and move back**: An attempt is made to remove the virus from the file. If this succeeds, the cleaned file is moved back to its original location on the respective client. If the virus cannot be removed, the file is not moved back.
- **Quarantine: Move back**: Moves the file from the quarantine folder back to the client. ***Warning***: The file is restored to its original state and is still infected.

- **Quarantine: Send to Internet Ambulance**: If you discover a new virus or an unknown phenomenon, please always send us this file via the quarantine function of *G Data AntiVirus*. We will analyse the virus and send you a countermeasure as quickly as possible. Naturally our ***Emergency AntiVirus service*** will handle the data you sent with the utmost confidentiality and discretion.
- **Delete**: Deletes the selected reports. If reports to which a quarantine file belongs are to be deleted, you must confirm the deletion once more. In this case, the files found in quarantine are also deleted.
- **Delete dependent reports**: If, due to different tasks or tasks that were performed multiple times, a virus alert or a report is displayed twice or more, you can delete the duplicate from the log file using this option.

Update

This function updates the view. Loads the current ***reports*** from the ManagementServer.

Delete reports

This function deletes the selected reports. If reports to which a ***Quarantine*** file belongs are to be deleted, you must confirm the deletion once more. In this case, the files found in quarantine are also deleted.

Print

Use this function to start the print procedure for reports. In the selection screen that appears, you can specify which details and areas you would like to print.

Page view

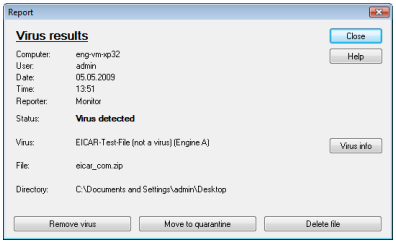
Using the page preview function you can obtain a preview of the page to be printed on the monitor before actually printing it out.

Remove virus

Using this function you can attempt to remove the virus manually from the original file. The success or otherwise of this attempt is indicated in the overview.

Move to quarantine

This function moves the selected files into the quarantine folder. The files are encrypted and saved in the ***quarantine*** folder on the ManagementServer. The original files are deleted. The encryption ensures that the virus cannot cause any damage. Please ensure that for each quarantined file there is a corresponding report. If you delete the report the quarantined file is also deleted. You can send a file from the quarantine folder for examination by the ***Emergency AntiVirus service***. To do this, double-click on the quarantine report.



In the report dialogue, click the button **Send to the Internet ambulance** after entering the submission reason.

Delete file

With the function **Delete file**, you delete the original file on the client.

Move back file from quarantine

Moves the file from the ***quarantine*** folder back to the client.

? ***Warning***: The file is restored to its original state and is still infected.

Clean file and move back out of quarantine

The virus is removed from the file with this function and the cleaned file is moved back to the client. If the virus cannot be removed, the file remains in the ***quarantine*** folder.

Show options

With a large number of different reports, it is useful to show and list these according to particular criteria. The following options are available:

Hide dependent reports: If, due to different jobs or jobs that were performed multiple times, a virus alert or a report is displayed twice or more, you can hide the duplicate using this option. Only the most current entry is then shown and can be edited.

Hide archived files

Show all reports

Show all reports with unremoved viruses

Show all quarantine reports

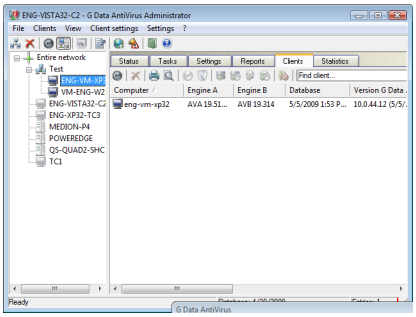
Show quarantine contents

Show all HTTP reports

Show all firewall reports

Clients

In the ***Client selection area*** select a group to obtain an overview of all group clients. For each client, the versions that the installed components have will be displayed along with the last time the client reported to the ManagementServer. Here, it can be verified whether the clients are running correctly and whether Internet updates have been performed.



In the **clients** task area, the following information is available in a list. It can be sorted according to different criteria by simply clicking on the corresponding column name. The column according to which current sorting is carried out, is indicated by a small arrow symbol. The following criteria are available:

- **Computer**: The name of the client concerned is identified here.
- **Engine**: The version number of the virus database and the date of its last update via Internet update are displayed here.
- **Data status**: The date on which the status of the virus database was updated on the client. This date is not identical with the update date of the virus database.
- **Version G Data AntiVirus Client**: Here you will find the version number and the creation date of the utilised *G Data AntiVirus Client software*.
- **Last access**: This entry lets you know when the *G Data AntiVirus Client* was last active.
- **Update virus database**: Here you can determine whether the update to the most current virus database is *completed*, whether a job has been issued to carry this out or whether there were irregularities or errors.

- **Update program files**: If new updates of the client software occur, you receive the corresponding status information here.
- **Date**: The date on which the status of the program files was updated on the client.
- **Exception directories**: If you have created exception directories that are not to be incorporated in the virus monitoring, the corresponding ***Existing exceptions*** are displayed here.

? In the menu bar, an additional menu entry named **Client settings** is available with the following functions for the task area **Clients**:

- **Install G Data AntiVirus Client**: Installs the client software. The installation is only possible if the clients meet certain requirements.
- **Uninstall G Data AntiVirus Client**: Commands the *G Data AntiVirus Client* to uninstall itself. For a complete removal, the client computer must be restarted. The user is prompted to do this by a message.
- **Install G Data AntiVirus Client for Linux**: You can also install special client software on Linux clients in the network. For more information please read the section ***Installation of the client software on Linux computers*** in the annex of this documentation.
- **Assign G Data subnet server**: While you have the option of assigning specific ***subnet servers*** to clients with the function **Manage server**, you can also select a subnet server targeted for the respective client via the function **Assign G Data subnet server**.
- **Reset to default settings**: For the protection of the entire network or selected groups, you can create ***Default settings*** and by so doing, quickly assign standardised procedures for virus protection. In order to bring individual rules for single groups back to the general state, you can reset the default settings to the globally defined standard values with this function.
- **Update virus database now**: Updates the virus databases on the clients with the files from the ManagementServer.
- **Automatically update virus database**: Switches on the automatic update of the virus database. Clients periodically check whether a new version is available on the ManagementServer and execute an automatic update.

- **Update program files now**: Updates the program files on the clients with the files from the ManagementServer. A client reboot may be necessary after updating the program files.
- **Automatically update program files**: Switches automatic updating of program files on. Clients periodically check whether a new version is available on the ManagementServer and execute an automatic update.
- **Restart after update of program files**: As administrator, you can specify here what priority an update of the program files has on the clients. Thus using **Open client display window**, you can thus inform a user that he should restart his client computer at a convenient time, via **Create report** using the log files in the area **Reports**, or via **Perform restart without querying** automatically force a restart.

Update

This function updates the view and loads the current client settings from the ManagementServer.

Delete

You can remove a client from a ***group*** here.

Print

Use this function to start the print procedure for the client settings. In the selection screen that appears, you can specify which details and areas of the client settings you would like to print.

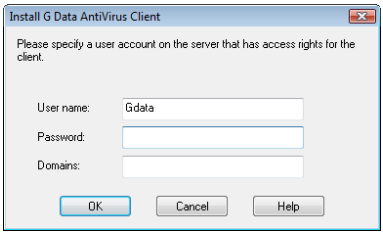
Page view

Here you can, prior to the actual print out, output a preview of the page to be printed to the monitor.

Install G Data AntiVirus Client

Installs the *G Data AntiVirus Client software*. The installation is only possible if the clients meet certain requirements.

Clients can also be configured from the ***ManagementServer*** using the *G Data AntiVirus Client software*, as long as they meet certain prerequisites. Activating this function opens a menu in which you enter access data for the server via which installation of the *G Data AntiVirus Clients* should be carried out.



After entering the relevant data (which is saved by the program so it does not need to be reentered every time), please confirm by clicking **OK**. A dialogue box then opens in which all available clients are displayed. Select one or more disabled clients here, then click on **Install**. *G Data AntiVirus* then automatically installs the client software on the relevant computer. If the software cannot be installed using the ***remote installation*** described here, you can also install it on the client manually or semi-automatically.

? To be able to access ***disabled clients***, they must of course also be displayed in the directory display. When the **Install AntiVirus Client** function is being used, the program informs you of this as necessary and enables displaying of the disabled clients.

? You can also install special client software on ***Linux clients*** in the network. For more information please read the section ***Installation of the client software on Linux computers*** in the annex of this documentation.

Uninstall G Data AntiVirus Client

Commands the *G Data AntiVirus Client* to uninstall itself. For complete removal the client must be restarted. The user is prompted to do this by a message.

Update virus database

Updates the virus database on the client with the files held on the ManagementServer.

Automatically update virus database

Switches on the ***automatic update of the virus database***. Clients periodically check whether a new version is available on the ManagementServer and execute an automatic update.

Update program files

Updates the program files on the client with the files held on the ManagementServer. A client reboot may be necessary after updating the program files.

Automatically update program files

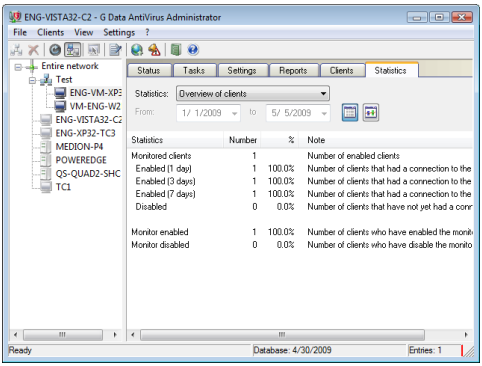
Switches automatic updating of program files on. Clients periodically check whether a new version is available on the ManagementServer and execute an automatic update.

Process directory exceptions

You can define client directory exceptions here that are not to be checked during the execution of scan jobs.

Statistics

In this task area, you can permit the display of statistical information about virus occurrences and client infections. Under **Statistics**, simply select whether you would like a general overview of the clients and their interaction with the ManagementServer (**Overview of clients**), an overview of viruses against which protection was provided (**Virus hit list**) or a listing of the infected clients (**Infected clients hit list**).


ENG-VISTA32-C2 - G Data AntiVirus Administrator
File Clients View Settings ?
Entire network
Test
ENG-VM-XP3
VM-ENG-W2
ENG-VISTA32-C2
ENG-XP32-TC3
MEDION-P4
POWEREDGE
QS-QUAD2-SHC
TC1
Status Tasks Settings Reports Clients Statistics
Statistics: Overview of clients
From: 1/ 1/2009 to 5/ 5/2009
Statistics Number % Note
Monitored clients 1 Number of enabled clients
Enabled (1 day) 1 100.0% Number of clients that had a connection to the
Enabled (3 days) 1 100.0% Number of clients that had a connection to the
Enabled (7 days) 1 100.0% Number of clients that had a connection to the
Disabled 0 0.0% Number of clients that have not yet had a conn
Monitor enabled 1 100.0% Number of clients who have enabled the monit
Monitor disabled 0 0.0% Number of clients who have disable the monito
Ready
Database: 4/30/2009
Entries: 1

G Data AntiVirus Client

The ***client software*** provides the virus protection for the clients and runs ManagementServer jobs in the background without a user interface. The clients possess their own virus signatures and their own scheduler so that virus analyses can also be run in offline mode (e.g. for notebooks).

Installation of the clients

The ***client software*** provides the virus protection for the clients and runs ManagementServer jobs in the background without a user interface. Installing the client software is generally done centrally by the administrator for all clients. A setup wizard in the administrator tool will help you do this.

If installation of the clients over the network should fail, you can install the client software directly on the client computers. To install the client on a client computer, please place the *G Data AntiVirus CD-ROM* in the client computer's CD-ROM drive and press the **Install** button. Then select the **G Data AntiVirus Client** component by clicking on the adjoining button.

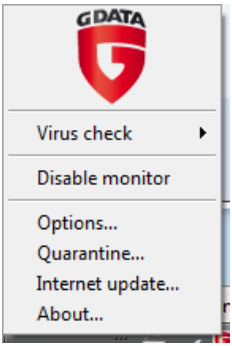
During installation, enter the ***server name*** or ***IP address of the server*** on which the ManagementServer is installed. The server name is required so that the client can communicate with the server over the network. Furthermore, you must enter the ***computer name*** for this computer if this is not automatically displayed.

? To install clients for Samba file servers, please read the following section in the annex of this documentation: ***Installation of client for Samba file server***

Security icon

After the installation of the client software, an icon in the taskbar is available to the user of the client so that he can check his system for viruses independently of administrative specifications.

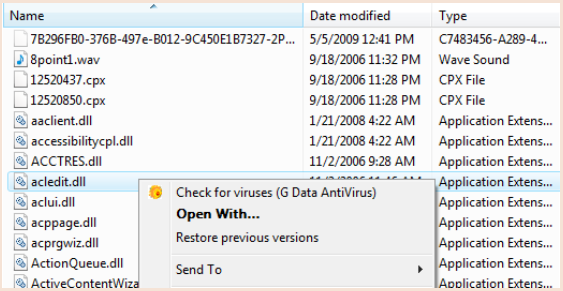
Using the ***right mouse button*** he can click the *G Data AntiVirus Client symbol* to open a ***context menu*** which makes the following functionality possible for him:



Virus check

Via this function, the user can also carry out a targeted check using the *G Data AntiVirus Client* on his computer even outside the checking period specified by the administrator. Similarly, the user can check diskettes, CD-ROMs, memory and the autostart area, as well as targeted individual files or directories (folders) here. In this manner, notebook users who only rarely connect their computers to the company network can prevent virus infestation in a targeted manner. In addition, he now has the possibility to move virus-infected files to a local quarantine folder thus making them harmless and available to the network administrator at the next opportunity for further appraisal.

? The user can also easily check files or directories from Explorer by selecting the files or directories and utilising the function **Check for viruses (G Data AntiVirus)** in the ***context menu*** with the right mouse button.



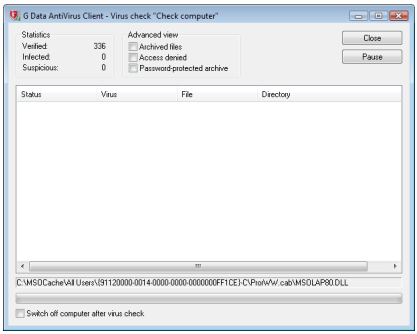
During an ongoing virus check, the context menu is expanded with the following entries:

- **Virus check priority**: The user has the option of determining the priority of the virus check here. If ***High***, the virus check is carried out quickly; although it can significantly slow down work with other programs on this computer. With the ***Low*** setting on the other hand, the virus check takes comparatively long but other work on the client computer is not significantly slowed.

- **Stop virus check**: This enables the user to interrupt the virus check and continue it again at a later time.

- **Cancel virus check**: As long as the administrator has enabled the option **User can change monitor options**, the client user can also cancel virus checking on his client even if the check was manually started on the client.

- **Display scan window**: With this option, the user can display the information window in which the course and progress of the virus check is displayed.



Disable monitor

Using this command, the *G Data AntiVirus Monitor* can be switched off by the user for a specified time (from ***5 minutes*** up to ***until the next computer restart***). This is only possible if the administrator has assigned the corresponding rights. For example, the temporary switching off of the monitor may be useful during extensive file copying procedures as this would considerably speed the process up. Virus checking is also switched off during this interval. This should be borne in mind.

Options

As long as the administrator has enabled the option **User may change monitor options**, the user can adjust the client options for virus checking on his computer as well as the options for the monitor which runs in the background to meet his own requirements.

? ***Warning***: Of course this way it would be possible to effectively turn all virus control mechanisms on the client off. As an administrator you should only make this option available to technically competent users.

? The security relevant settings under **Options** can also be password-protected for the client computer. Accordingly the administrator assigns the relevant client an individual password, with which the user can change the virus control functions on the client. This password is granted via the work area **Settings** in the Administrator under **Password protection for changes to options** .

The individual setting options that are available to the user in the area **Options** are explained in detail in the area ***Administrator program setup > Task areas > Settings*** in the following sections:

- **Monitor**
- **Email**
- **Virus check**
- **Web/IM filter**
- **Spam filter**

? If you activate the option **The user can run virus checks** for the user on his client, he can check his client computer for viruses independently of the monitor's automatic virus control. The settings that are possible here for the user on the client correspond to the greatest possible extent to those found in the **Monitor** application.

Quarantine

Even computers which are not currently connected to the network monitored by *G Data AntiVirus*, have a local quarantine folder available to them. This means that users who are not in the office (e.g. during business travel) can place suspicious files in quarantine and then have them checked at the next available opportunity within the company network. You can disinfect infected files in the quarantine folder, or if this is not successful, delete them and, if necessary, move them back from the quarantine to their original location.

? ***Warning***: Moving back does not remove the virus. You should only select this option if the program cannot run without the infected file and you nevertheless need it for data recovery.

Internet update

The *G Data AntiVirus Client* can also be used to carry out independent Internet virus signature updates from the client computer. This makes sense for e.g. notebooks that occasionally do not have access to the corporate network. This feature can be specifically enabled for individual clients by the administrator.

? Use the **Settings and scheduling** button to run scheduled virus signature updates on the client.

About

Under **About** you can find out the version and up-to-dateness of the virus database.

G Data AntiVirus WebAdministrator

The *G Data AntiVirus WebAdministrator* is web-based administration software for the ManagementServer. It can be launched via a ***web browser***.

Installation of the WebAdministrator

The ***WebAdministrator*** is web-based administration software for the ManagementServer. It can be launched via a ***web browser***. When installing the WebAdministratoryou may be asked to install ***Microsoft .NET Framework components***. These are essential for the operation of the WebAdministrator. After the installation you will need to restart the computer.

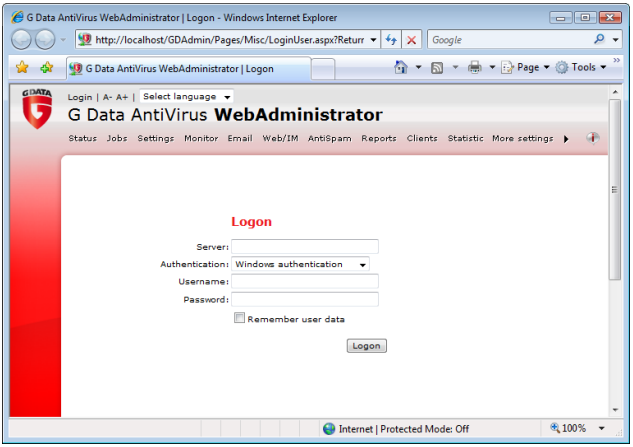
? ***Warning***: BEFORE installing the WebAdministrator you need to enable the ***Compatibility with IIS Metabasis and IIS 6 Configuration*** Windows function. If this function is not available, installation of the WebAdministrator will be cancelled. This setting can be found, for example, in Windows Vista under ***Start > Control panel> Programs > Programs and Functions > Switch Windows Functions on or off***. You can switch the setting on or off here in ***Internet information services > Web administration tools > Compatibility with IIS 6 management > Compatibility with IIS Metabasis and IIS 6 Configuration***. Furthermore the ***www services*** must also be enabled, if this has not already been done. To do this, please check the box in ***Internet information services > www services***.

You can now install the WebAdministrator.

After the installation you will see the icon for the ***G Data AntiVirus WebAdminstrator*** on the desktop of your computer.

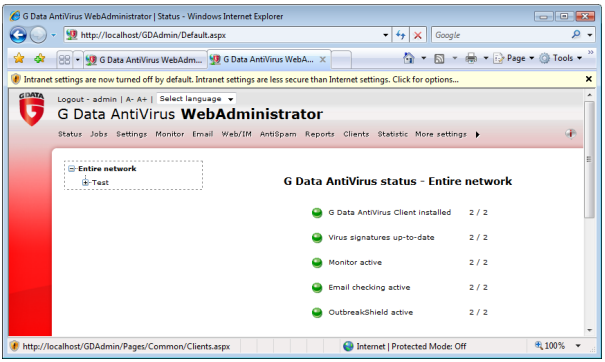
Program setup of the WebAdministrator

To use the ***WebAdministrator***, just click on the WebAdministrator desktop icon. Your web browser will then open automatically at a login page for accessing the WebAdministrator.



As with your usual ***Administrator*** enter your ***Access data*** then click on the **Log in** button.

WebAdministrator functionality corresponds as closely as possible, in terms of content and operation, to the standard ***G Data AntiVirus Administrator***.


G Data AntiVirus WebAdministrator | Status - Windows Internet Explorer
http://localhost/GDAdmin/Default.aspx
Intranet settings are now turned off by default. Intranet settings are less secure than Internet settings. Click for options...
Logout - admin | A- A+ | Select language
G Data AntiVirus WebAdministrator
Status Jobs Settings Monitor Email Web/IM AntiSpam Reports Clients Statistic More settings
Entire network
Test
G Data AntiVirus status - Entire network
G Data AntiVirus Client installed 2 / 2
Virus signatures up-to-date 2 / 2
Monitor active 2 / 2
Email checking active 2 / 2
OutbreakShield active 2 / 2
http://localhost/GDAdmin/Pages/Common/Clients.aspx
Internet | Protected Mode: Off
100%

Attachment

Troubleshooting (FAQ)

Here you can find answers to questions which may arise while you are working with *G Data AntiVirus*.

I want to execute client installation centrally from the server via the Administrator

The most convenient way to run the installation is via the ***Administrator***. However, to do this, the clients must meet certain prerequisites. ***Remote installation*** can be completed in two ways. If the client meets the necessary prerequisites, the files are copied directly and entries made in the registry. With Windows XP professional, Windows Vista and Windows 2000 the *G Data Client* is started immediately. If the server can only access the hard drive and not the registry, or if other system prerequisites are not met, the entire set-up program is copied to the client and started automatically at the next computer reboot. To install, simply access the Administrator menu bar and choose the ***Clients > Install G Data AntiVirus Client*** function. An input window appears in which you should enter the user name, password and domain for the ManagementServer. After this data is entered a window appears showing all available network computers. Activated clients are identified by a symbol. Disabled clients are represented by a greyed-out symbol. Select a network computer for installation and click on the **Install** button. The *G Data Client* is then installed on this computer. If your system does not meet the prerequisites for remote installation of the *G Data AntiVirus Client software*, you of course have the option of using the *G Data Client software* to install clients manually or semi-automatically.

I want to install the Administrator on a client computer

You can of course start the ***Administrator*** from any other computer in the network as well.

? For *G Data AntiVirus* to run smoothly, it is not essential to install the Administrator on the clients. Installing the Administrator on a client computer is actually only recommended if deemed necessary to solve a problem *on site*.

We recommend that the ***Admin*** directory is shared and then invoking the ***Admin.exe*** file from the other computer. Of course you can also copy the file to another computer and launch it from there. Directory sharing has the advantage that you are always launching the latest version, as the file can be updated via Internet update. Optionally you can also place the *G Data AntiVirus CD-ROM* in the CD-ROM drive on the client computer, press the **Install** button and then select the *G Data AntiVirus Administrator* components by clicking the corresponding button. In the following start screen, you are informed that you are about to install the Administrator on your system. Please ensure that you have now closed all open applications in your Windows system, as otherwise they may cause problems during the installation. Click on **Next** to continue with the installation. The next screen allows you to select the location where the Administrator data is to be saved. By default, the ManagementServer is stored under ***C: > Programs > G Data > G Data AntiVirus Administrator***. If you want to select a different storage location, you can use the **Browse** button to open a directory view where you can select or create a new directory. **Next** takes you to the next installation step. Now you can select a program group. If you click on **Next**, you will usually see the program in the ***G Data AntiVirus Administrator*** program group in the Windows start menu program selection screen. The installation ends with a completion screen. Click on **End**. You can now use the Administrator. You can invoke the Administrator tool for the control of the ManagementServer by clicking the entry ***G Data AntiVirus Administrator*** in the program group ***Start > Programs > G Data AntiVirus Administrator*** from the start menu.

I want to configure the clients using the G Data AntiVirus CD-ROM with the client software

You can also install the client software directly on individual clients using the supplied CD. Place the ***CD-ROM*** in the CD-ROM drive on the client computer, then select the ***G Data AntiVirus Client*** component by clicking on the button next to this. During the installation you will be asked for the name of the computer on which the ManagementServer is installed. Enter the corresponding name (e.g. ***avk_server***). Click on the **Next** button to complete the installation. If the Setup program asks for a computer restart on the completion screen, please do so as the client will only become functional after a restart.

Some clients report that "The virus database is corrupted.". What can be done?

In order to ensure optimal virus protection, the integrity of the virus database is regularly checked. If an error occurs, the report ***The virus database is corrupted*** is included. Delete the report and download the current update of the virus database from our server. Subsequently perform an update of the virus database on the affected clients. Please contact our telephone hotline if the error report is included again.

The clients are to be addressed via their IP addresses, not their names.

Installation of the ManagementServer: The server name will be requested during the installation. The name must be replaced by the ***IP address***. You can also replace the server name later by the IP address if the ManagementServer is already installed. Adjust the registry entry ***HKEY_LOCAL_MACHINE\Software\G Data\G Data AntiVirus ManagementServer\ComputerName*** and the file ***\Programme\G Data\G Data AntiVirus ManagementServer\AvkClientSetup\RegServer.txt*** for this purpose.
Activation of the clients in the administrator: In order that the connection from the server to the clients can also be established via the IP address, the clients must be activated in the administrator with their IP address. This can be done either manually (***activate clients/client (dialogue)***) or by searching an IP address space (***search for client/computer***). ***G Data AntiVirus client setup from the CD***: If the clients are installed directly from the ***CD***, the installation program asks for both the server name and the name of the computer. Enter the appropriate IP address here.

My mailbox was moved to the quarantine.

This can happen if an infected mail is found in the mailbox. ***File move back***: Close the mail program on the affected client and delete any possibly newly created archive file. Subsequently open the associated report with the administrator and click on ***Move file back***. Please contact our telephone hotline if moving back fails.

How can I check whether the clients have a connection to the ManagementServer?

The column **Last access** in the **Clients** task area contains the date on which the client last reported to the ManagementServer. Normally the clients report to the ManagementServer every few minutes (if there are no scan jobs currently running). The following reasons may cause a failed connection:

- The client is switched off or disconnected from the network.
- A TCP/IP connection cannot be established between the client and the ManagementServer. Check the network settings.
- The client cannot determine the IP address of the server, i.e., the name resolution is not functioning. The connection can be tested using the ***ping*** command. For this purpose, enter the command ***ping <server name>*** at the prompt, where ***<server name>*** is the name of the computer in the network on which the ManagementServer is installed.

Some clients report that "Program files have been changed or are corrupted". What can be done?

In order to ensure optimal virus protection, the integrity of the program files is regularly checked. If an error occurs, the report ***Program files have been changed or are corrupted*** is included. Delete the report and download the current update of the program files (*G Data AntiVirus client*) from our server. Subsequently perform an update of the program files on the affected clients. Please contact our telephone hotline if the error report is included again.

After client installation, some applications run significantly slower than before

The monitor oversees all file accesses in the background and checks the opened and saved files for viruses. This normally leads to a ***delay*** that is barely perceptible. If an application opens many files or opens some files very often, a significant delay can occur. In order to circumvent this problem, first disable the monitor temporarily in order to determine whether it is actually the cause of the delays. If the affected computer accesses files on a server, you must naturally also disable the monitor on the server. If the monitor is the cause, the problem can usually be remedied by defining an ***exception*** (= files that are not to be checked). For this purpose, the files that are frequently accessed must be identified. You can identify this data

with a program such as ***MonActivity***. If necessary, contact our ***ServiceCenter***. Known delays:

- When using some ***HP printers*** with ***Microsoft Office***, the files ***HP*.INI*** should be defined as an exception.
- When using the mail software ***Eudora***, the files ***EUDORA.INI*** and ***DEUDORA.INI*** should be defined as exceptions.

? Naturally you can also increase performance by not using both engines for virus checks but rather only one engine.

Installation of the client software on Linux computers

The product makes it possible to use ***G Data virus protection*** on ***Linux workstations*** of various distributions. The ***Linux client*** can thus (as with ***Windows clients***) be linked into the *G Data ManagementServer* infrastructure, centrally managed via the *G Data Administrator software* and supplied with signature updates. Analogous to the Windows clients, a file system monitor with a graphical user interface will be set up with Linux clients that orients itself to the Windows version in terms of functionality. For Linux computers that operate as ***file servers*** and provide Windows authorisations to different clients (via the ***SMB protocol***), a module can be installed that controls access to the cleared areas and carries out a file scan with every access event, so no malware can migrate from the Samba server to the Windows clients (or vice versa).

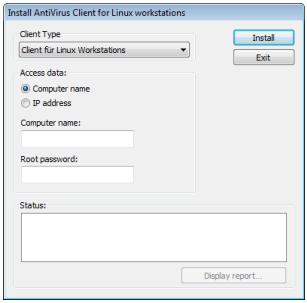
? For the ***Workstation client*** a kernel version equal or greater than 2.6.25 is required; for example, this is the case with Ubuntu 8.10, Debian 5.0, Suse Linux Enterprise Desktop 11, and other current distributions. A customisation is required in isolated cases with other distributions. The ***file server client*** can be used on all prevalent distributions.

In order to install the software on the Linux client, proceed as follows:

1 ***Remote installation of the client software over the network***

In the task area **Clients** in the menu **Client settings** select the command **Install G Data AntiVirus client for Linux** . A dialogue window appears through which you can define the client on which

the client software is to be copied. For this, the computer must be recognised in the network.



2 Use the selection **computer name** if a ***Samba service*** is installed on the client computer or if the computer is registered in the network's ***name server***. If the name of the computer is not recognised, use the computer's **IP address**.

3 Now enter the computer's **root password**. A root password must be allocated for a remote installation. By default, this is not the case with certain distributions, for example, Ubuntu.

4 Now click on the **Install** button. In the **Status** area, you can see if the installation of the client software was successful.

? ***Manual installation of the client software***

The following files can be found in a special directory on the program CD

- **installersmb.bin** = Installer for Samba file server
- **installerws.bin** = Installer for workstation

You can copy these files to the client computer and start the corresponding file to install the client software. In addition, you will also find a file here with the ***virus signatures***. The installation of this file is optional since the software automatically obtains the latest virus signatures from the server after the installation:

- **signatures.tar** = Archive with virus signatures

Linux file server clients: No connection with ManagementServer has been made / signatures will not be updated

1 Check whether both processes of the *G Data AntiVirus Client* are running: Enter the following via the command line

linux:~# ps ax|grep av

. You should receive the following

... Ssl 0:07 /usr/sbin/avkserver --daemon
... Ssl 0:05 /usr/sbin/avguard --daemon

responses. You can start the processes independently of the distribution used with

linux:~# /etc/init.d/avkserver start
linux:~# /etc/init.d/avclient start

and stop them with

linux:~# /etc/init.d/avkserver start
linux:~# /etc/init.d/avclient start

. To do this you must be logged in as the administrator (=“root“) on the Linux computer.

2 To view the log files see:

The log files ***avk.log*** and ***remote.log*** are stored under ***/var/log/avk***. In the file ***avk.log*** the scan results of the scanner ***avkserver*** are logged, while in the file ***remote.log*** you can view the output from the ***avclient*** process, which creates the connection to the *G Data AntiVirus ManagementServer*. Look at the files and search for any error messages. If you wish to see more messages, then in the configuration files ***/etc/gdata/gdav.ini*** und ***etc/gdata/avclient.cfg*** set the entries for ***LogLevel*** to value ***7***.

Attention: A high LogLevel generates a lot of messages and causes the log files to quickly increase in size. Under normal operating conditions, always set the LogLevel to a low value!

3 Test the scanner.

Use the command line tool ***avkclient*** to test the functioning of the scan server ***avkserver*** . The following commands can be executed:

linux:~$ avkclient avkversion - outputs the version and latest update date of

the virus signatures

linux:~$ avkclient avkversion - outputs the version in short format

linux:~$ avkclient scan:<file> - scans the file ***<file>*** and outputs the result

4 Check the configuration file.

The file ***etc/gdata/avclient.cfg*** is the configuration file for the remote client ***avclient***. Check whether the address of the main management server (MainMMS) is entered correctly. If not, delete the incorrect entry and log the Linux client via the *G Data AntiVirus Administrator* on again or enter the address of the *G Data AntiVirus ManagementServer* directly.

5 Test your authorisations.

Virus protection for the Samba authorisations is enabled via the entry

vfs objects = gdvfs

in the Samba configuration file ***/etc/samba/smb.conf***. If the entry is in the section ***[global]***, then protection is enabled for all authorisations; if the line is in another section, then the protection is only for the corresponding authorisation. You can comment out the line for test purposes (by entering a hash symbol "#" at the start of the line), to determine whether access functions without virus protection. If not, then please first search for the error in your Samba configuration.

6 ***Linux workstation monitor***

Check whether the monitor process ***avguard*** is running:

ps ax|grep avguard

The monitor requires the kernel module ***redirfs*** and ***avflt***. With ***lsmod*** you can check whether the modules are loaded: ***lsmod|grep redirfs*** and ***lsmod| grep avflt***....

The modules would have to be compiled for the kernel used by you.

This is taken care of by the ***Dynamic Kernel Module System*** (***DKMS***), which must be installed together with the matching kernel header packages of your distribution. If this is the case, DKMS compiles and installs the modules automatically. You will find the ***log file*** of the monitor under***/var/log/gdata/avguard.log***.

How do I protect myself against malware?

Although ***G Data software*** not only detects and removes known viruses, it also detects thus far unknown malware with the aid of the heuristic analysis; it is undoubtedly better to eliminate a virus infection at the outset. To this end, certain security precautions that don't require a lot of effort, yet noticeably increase the security of your system data should be undertaken.

- ***Use user accounts***: You should use two user accounts on your computer. An ***administrator account***, which you always use for installing software or carrying out basic settings on your computer, and a ***user account*** with limited rights. The user account, for example, should not be able to install programs or undertake modifications in the Windows operating system. You can use this account to, for example, surf the Internet in relative safety, transfer data from other computers, etc. How you can set up different user accounts is explained in your Windows operating system's help documentation.

- ***Ignore spam email***: Chain letters and spam email should never be responded to. Even if such email does not contain a virus, its unwanted transmission significantly increases the flow of data in the Internet.

- ***Check suspected viruses***: If you have a confirmed suspicion of a virus, e. g. because newly installed software is not doing what it is supposed to do or an error message is displayed, check the relevant program for viruses, ideally before restarting the computer. This is a good idea, since, for example, certain Trojan horses only execute their delete commands during the next computer restart; therefore they are easier to identify and fight beforehand.

- ***Regular Windows updates***: It should also become routine to download the current patches from Microsoft, since these often close newly-detected vulnerabilities in Windows before a virus programmer has even had the idea of exploiting these using new malicious programs. Windows updates can also be automated.

- ***Use original software***: Even though storage media used for original software may be infected with viruses in very rare cases, the probability of a virus infection from pirated copies or copies stored on rewritable storage media is considerably higher. Therefore, only use original software.

- ***Treat software from the Internet with caution***: You should also exercise extreme caution when downloading software and only use software you really need and that originates from trustworthy sources. Never open files received by email from unknown persons or sent unexpectedly by friends, colleagues, or acquaintances. Ideally, make sure that you can start the respective application safely by first checking with the relevant authority.

? If you would like to delve into the problem of viruses, you will find interesting articles and information in the ***G Data virus encyclopaedia*** at: ***www.antiviruslab.com***

Notes

Index

A

About 74
Access data 21, 76
account type 25
Activate 20
Activate client 29, 35
Activate client (dialogue) 29, 35
Activate client/clients (dialogue) 79
activated 29
activated clients 29
Activation of the clients in the administrator 79
Add 27
Admin 77
Admin.exe 77
Administrator 6, 11, 17, 18, 19, 23, 76, 77, 81
Administrator account 85
Administrator program setup 23
Administrator software 11, 13, 81
Adware 42, 50
After client installation, some applications run significantly slower than before 80
Alarm notifications 33, 35
Analysis scope 39, 45
AntiSpam 58
Append report to outgoing email 55
Append report to received, infected mails 55
Archive scan 42
Archives 42
Assign clients 25
Assign G Data subnet server 64
Asterisk symbol 53
Attachment 77
Attention 83
Authentication 19
authorisations 25
Automatic installation of the client software 22
Automatic type recognition 42, 50
Automatic updates 31
Automatic updating of the virus database 68
Automatically clean 34
Automatically install client software on the enabled computers 20
Automatically update program files 47, 64, 68
Automatically update virus database 64, 68
Autostart function for your CD/ROM drive 11
avk.log 83
avk_server 78
avkclient 83
AvkClientSetupPck.exe 30
avkremote 83
avkremote packets 81
avkserver 83
avkvfs modules 81
avkvfs packet 81
Avoid browser timeout 57

B

BIOS 7
Boot scan 6, 7, 11, 50
Boot scan using the program CD 7
Boot scan with G Data software that you have downloaded from the Internet 7
Boot sectors 42, 50
Both engines - performance optimised 42
Browse 77

Business Sales 3

C

Cancel virus check 71
Carry out periodic update 31
CentOS 81
Check archive 50
Check email archives 50
Check emails before sending 55
Check for diallers / spyware / adware / riskware 42, 50
Check for viruses (G Data AntiVirus) 71
Check network access 50
Check received mails for viruses 55
Check suspected viruses 85
Check system areas on media exchange 50
Check system areas on system start-up 50
Check unread mails on program start-up (Microsoft Outlook only) 55
Check when writing 50
Clean file and move back out of quarantine 63
Client 11, 29, 30, 47, 54, 68, 70, 71, 74, 77, 78, 80
Client (activated) 37
Client (disabled) 37
Client and server software 6
Client for Samba file server 81
Client functions 48
Client selection area 23, 37, 38, 46, 50, 64
Client settings 24, 64
Client setup from the CD 79
client software 6, 11, 31, 64, 67, 70, 77
client symbol 70
Client version 64
Clients 13, 22, 24, 25, 27, 30, 38, 39, 64, 67, 80
Clients task area 31
command line 81
Comment 47
Compatibility with IIS Metabasis and IIS 6 Configuration 75
Components 11
Computer 20, 39, 59, 64
Computer name 15, 70, 81
Computer/group 25
Context menu 47, 70, 71
Create AntiVirus Client installation packet 30
Create boot CD 11
Create client installation packet 22
Create report 47, 64

D

Daily 42
Data media 39
Database 64
Database server 15
Database type configuration 17
Date/time 59
Debian 81
Default settings 21, 28, 64
Delay 80
Delete 28, 66
Delete attachment/text 55
Delete default settings 28
Delete dependent reports 59
Delete file 59, 62
Delete infected file 50
Delete reports 61
Delete scan jobs 45
DEUDORA.INI 80
DHCP 7

Diallers 42, 50
Directory 53
disable 28, 35
Disable monitor 72
disabled clients 29, 67
Disinfect (if not possible: delete file) 50
Display disabled clients 28, 29, 35
Display group jobs in detail 39, 45
Display local quarantine 48
Display log 25, 35
Display scan window 71
Domains 32
Download size limit 57
Drive 53

E

Edit group 27
Email 21, 33, 54, 59, 73
Email archives 42
Email notification 21, 34
Email protection 56
email security 48
Email settings 21, 33
Emergency AntiVirus service 13, 21, 33, 42, 59, 62
End 27
End IP address 29
Engine 64
Entire network 28
Eudora 80
EUDORA.INI 80
Exception 80
Exception directories 64
Exception directories for scan jobs 49
Exceptions 53
Existing exceptions 64
export 25

F

False alarm 50
Fedora 81
File 20, 24, 53
File / mail 59
File move back 79
File moved to quarantine 59
File server 81
File server client 81
File types 42, 50
Firewall 11, 30, 48, 67
Firewall reports 63
Folder 53, 59

G

G Data AntiVirus 77
G Data UpdateServer 31
G Data virus protection 81
General 2, 47
Group 27, 37, 39, 50
Groups 35, 49

H

Hard disk 53
Help 2, 35
Heuristics 42, 50
Hide archived files 59, 63
Hide dependent reports 59, 63
Host IDs 29
Hotline 2
How can I check whether the clients have a connection to the ManagementServer? 80
How do I protect myself against malware? 85
HP printer 80

HP printers 50
HP*.INI 80
HTTP reports 63
HTTP web content 57

I

I accept the terms of the licence agreement 14
I want to configure the clients using the CD-ROM with the client software 78
I want to execute client installation centrally from the server via the Administrator 77
I want to install the Administrator on a client computer 77
Icon in the taskbar 47, 70
Ignore spam email 85
IMAP 54, 56
Immediately transfer new reports to the main server 35
In case of an infection 42, 55
Incoming mails 55
Infected archive 42, 50
Infected clients hit list 69
Inform user when a virus is found 56
Initial program launch (Setup wizard) 20, 24
Install 11, 13, 16, 20, 67, 70, 77, 81
Install a main server 14
Install a secondary server 14
Install a subnet server 14
Install client 22, 64, 67
Install G Data AntiVirus Client for Linux 81
Install G Data AntiVirus Client for Linux 64
Installation 11
Installation completion 17
Installation of client for Samba file server 70, 81
Installation of the Administrator 18
Installation of the client 70
Installation of the ManagementServer 13, 79
Installation of the WebAdministrator 75
Installation via the Administrator 77
Instant Messaging 58
Instant Messaging (integration into IM application) 58
Integrated authentication 19
integrated database 15
integrated login 25
Internet connection 16
Internet content (HTTP) 57
Internet Explorer 32
Internet Explorer connection data 32
Internet update 2, 7, 16, 21, 30, 31, 35, 74
IP address 79, 81
IP address of the server 70
IP addresses 29

J

Job 42
Jobs 24, 29, 38, 39

L

Last access 64, 80
Last run 39
Licence agreement 3, 14
Limit 34
Linux client 81
Linux clients 23, 67
Linux computer 7
Linux computers 81
Linux workstation monitor 83

Linux workstations 81
log entries 34
Log file 25
Log in 76
Log view 25
Login data and settings 30, 31, 32
LogLevel 83
Logon 19
Logs 45

M

Mail plug-in 59
Mail server 21
Main MMS 14
Main server 14, 25
Manage server 25, 64
ManagementServer 2, 6, 7, 11, 13, 14, 18, 31, 67, 81
ManagementServer also as subnet server 14
ManagementServers 81
Master boot records 42
Media exchange 50
Menu bar 23, 24, 35
Microsoft .NET Framework components 75
Microsoft Messenger (version 4.7 and later) 58
Microsoft Office 50, 80
Microsoft Outlook 54
Microsoft SQL Express 15
MonActivity 80
Monitor 6, 21, 29, 42, 50, 59, 72, 73, 83
Monitor exceptions 53
monitor options 48
Monitor ports 56
Monitor status 50
Monthly scan 42
Move back file from quarantine 63
Move file back 79
Move file to quarantine 42, 50, 59
Move to quarantine 62
Multi-user and network licences 2
My mailbox was moved to the quarantine. 79

N

Name 15, 39
Name of your computer 15
Name server 81
Network icon 37
New group 27, 35
New scan job (periodic) 41
New scan job (single) 41
Non-selectable devices 37
Notebooks 31
Notes 87
Notify clients of option changes from the server 35

O

On system start 42
one-time scan job 39
Online database for frequently asked questions (FAQ) 2
Online registration 2, 6, 16, 30, 32
online registration form 2
Online virus encyclopaedia 35
only in the first session 47
Only show completed scan jobs 45
Only show open scan jobs 45
Only show periodic scan jobs 45
Only show single scan jobs 45
Open client display window 47, 64
openSUSE 81

Options 73
Other program starts (access password) 23
OutbreakShield 56
Outgoing emails 55
Outlook 50, 55, 56
Overview of clients 69

P

Page preview 26, 62, 66
Partition 53
Password 16, 19, 25, 32
Password protection for changes to options 48, 73
Perform restart without querying 64
periodic scan jobs 39
ping 80
Plug-in 54
POP3 54, 56
Port 33
Port addresses 58
Port number 21
PremiumHotline 2
PremiumSupport 3
PremiumSupport extensions 3
Print 25, 26, 61, 66
Print templates 26
Prior to installation 6
Priority scanner 42
Procedure 25
Process directory exceptions 68
Process IM content 58
Process Internet content (HTTP) 57
Processors 42
Program files 31
Program files have been changed or are corrupted 80
Program interface 38
Program setup of the WebAdministrator 76
Properties 41
Protect Microsoft Outlook through an integrated plug-in 56
Proxy server 32
Proxy settings 31

Q

quantity limit 21
Quarantine 13, 42, 48, 50, 59, 61, 62, 63, 74
Quarantine folder 59
Quarantine: Clean and move back 59
Quarantine: Move back 59
Quarantine: Send to Internet Ambulance 59
Question mark symbol 53

R

Read / write 25
Read only 25
Recipient 34
Registration number 2, 16
regular scan job 39
Regular Windows updates 85
Regularly transmit scan progress to the server 42
Reject 50
Remote installation 6, 22, 67, 77
Remote installation of the client software over the network 81
Remote installation of the Linux software 81
remote.log 83
Remove 27
Remove virus 62
Remove virus from the file 59
Reporter 59

Reports 24, 34, 38, 59, 61, 64
Reset to default settings 64
Restart after update 47
Restart after update of program files 64
Restart without querying 47
Right mouse button 70
Riskware 42, 50
Rollbacks 34
Root password 81
Router 7
Run 11, 42
Run again (immediately) 39
Run scan jobs again (immediately) 45

S

Samba server 7, 23, 81
Samba service 81
Scan email for viruses 56
Scan folder for viruses 56
scan jobs 39, 59
scan logs 34
Scan options 56
Scanner 42
Schedule 39
Scheduling 39
Search for client/computer 79
Search for computer 29
second server 14
Secondary MMS 14
Security icon 70
Select server type 14
Send alarm notifications by email 34
Send to the Internet ambulance 62
Sender address 21
Server 18, 19, 23
Server (activated) 37
Server (disabled) 37
Server names 70
Server settings 34
Server type structure 14
ServiceCenter 3, 80
Settings 21, 24, 28, 30, 34, 35, 38, 42, 46, 50, 73
Settings and scheduling 48, 74
Setup wizard 6, 20, 24
Setup/LinuxClient/Debian 81
Setup/LinuxClient/Fedora 81
Setup/LinuxClient/Suse 81
Show all firewall reports 63
Show all HTTP reports 63
Show all jobs 45
Show all quarantine reports 63
Show all reports 63
Show all reports with unremoved viruses 63
Show content of the quarantine folder 63
Show options 45, 63
Single scan jobs 39
SLE 81
SMB Protocol 7, 81
SMTP 21, 54, 56
SMTP server 33
Software CD 11
Some clients report that "Program files have been changed or are corrupted". What can be done? 80
Some clients report that "The virus database is corrupted.". What can be done? 79
Spam filter 58, 73
Special feature for scan jobs on a Linux file server 45
Special feature on a Linux file server 49
Spyware 42, 50

SQL database 14, 17
SQL server 15
Standard ports 56
Start IP address 29
Start menu 11
Start screen 13
Start update now 31
Starting the installation 16
Statistics 38, 69
Status 38, 39, 54, 59, 81
Stop virus check 71
Subfolders 53
Subnet server 35
Subnet server synchronisation 26
Subnet servers 25, 64
Synchronisation 35
System 7
System areas 42
System requirements 7

T

Target folder 14
Task areas 23, 30, 38
TCP/IP 13
TCP/IP layer 54
TCP/IP protocol 7
The clients are to be addressed via their IP addresses, not their names. 79
The user can change email and monitoring options 48
The user can change the firewall options 48
The user can download signature updates 48
The user can run virus checks 48, 73
The virus database is corrupted 79
Time 25, 42, 64
Time / scheduling 42
Time interval 39
T-Online 50
Toolbar 23, 35
Tools 56
Treat software from the Internet with caution 85
Trillian (version 3.0 and later) 58
Troubleshooting (FAQ) 77
Turn computer off after virus scan if no user is logged on 42

U

Ubuntu 81
Uninstall client 64, 68
Until the next computer restart 72
Update 25, 28, 30, 31, 35, 41, 61, 66
Update complete 7
Update now 31
Update program files 64, 68
Update program files now 64
Update rollback engine A / B 34
Update settings 48
Update status 31
Update view 28, 35
Update virus database 64, 68
Update virus database now 64
Update virus signatures 34
Update virus signatures automatically 47
Updates 47
UpdateServer 7, 11, 13, 16, 30, 31
Use all available processors 42
Use engines 42, 50, 56
Use original software 85
Use proxy server 32
Use spam filter 58
Use user accounts 85
User account 31, 47

User account and proxy settings 32
User management 19, 25
User may change monitor options 71, 73
User name 2, 19, 32
User names 16

V

Version check 32
Version information 55
Version number 2
View 24, 30, 39, 59
Virus 59
Virus check 48, 71, 73
Virus check priority 71
Virus checked by G Data AntiVirus 55
virus checks 25
Virus database 31
Virus detected 59
Virus encyclopaedia 35, 55
Virus hit list 69
Virus monitor 42, 50, 58
Virus news 55
Virus protection 2
Virus scanner 59
Virus signatures 7, 81

W

Warning messages 54, 56
Web / IM 57
Web browser 75
Web/IM filter 73
WebAdministrator 11, 75, 76
Weekdays 42
What do I do if my computer will not boot from the CD-ROM? 7
Wildcards 53
Windows authentication 19
Windows clients 81
Windows user 25
Windows user account 19
Windows user group 25
Windows version 11
Workstation client 81
www services 75